Japanese Patent Application Laid-Open No. 10-20956

[Title of the Invention] Software Accounting Method and System

[Abstract]

[Problem] It is an object to provide a software accounting method an system capable of collecting the amount of use proportional to the number of uses corresponding a function of using software.

[Means for Solution] When a user activates a software and transmits user information to an accounting center, the accounting center receives and acquires a rental fee for the software and a first decoding secret key, updates accounting information corresponding to an invoicee ID and transmits the first decoding secret key thus acquired to a user processor and user processor decodes and executes the whole or partial encoded region of the software by using the first decoding secret key received from the accounting center.

[Claims for Patent]

[Claim 1] A software accounting method for accounting a rental fee for a software to be provided to a user processor,

wherein an information providing system encodes a whole or partial software to be provided to an invoicee and distributes the software thus encoded to a user,

an accounting center registers, as registration information, a software identifier, a rental fee for the software and a first decoding secret key for decoding the

encoded software for each accounting object software,

the invoicee registers an invoicee ID to the accounting center,

when the invoicee activates the software and transmits a software use notice including the software ID to the accounting center,

the accounting center retrieves the rental fee for the software and the first decoding secret key based on the software use notice,

updates accounting information corresponding to the invoicee ID with the rental fee for the software, and

transmits the first decoding secret key thus acquired to the user processor, and

the user processor decodes and executes the whole or partial encoded region of the software by using the first decoding secret key received from the accounting center.

[Claim 2] The software accounting method according to claim 1, wherein the user processor generates a random number and transmits the random number together with the software use notice to the accounting center,

the accounting center receives the random number from the user processor and transmits the received random number together with the first decoding secret key to the user processor, and

the user processor receives the first decoding secret key and the random number from the accounting center, and

compares the generated random number with the received

random number and decides whether they are coincident with each other or not, and decodes the software only when they are coincident with each other.

[Claim 3] The software accounting method according to claim 1 or 2, wherein the accounting center further includes, as the registration information, a second secret key for encoding the first decoding secret key corresponding to the software, and transmits encoded information to be the encoded first decoding secret key to the user processor by using the second secret key, and

the user processor extracts the second secret key buried in the software,

decodes the encoded information to acquire the first decoding secret key by using the second secret key, and

decodes the software by using the first decoding secret key thus acquired.

[Claim 4] The software accounting method according to claim 1, 2, or 3, wherein the user processor encodes a part of information to be transmitted to the accounting center by using a third private secret key of an invoicee, thereby generating a sign to be transmitted to the accounting center, and

the accounting center further includes a public key corresponding to a third private secret key of the invoicee and decides whether or not information obtained by decoding the sign with the public key is coincident with other information received from the user processor, and

transmits the first decoding secret key to the user

processor only when they are coincident with each other.

[Claim 5] The software accounting method according to claim 1, 2, 3 or 4, wherein the user processor decodes the encoded software and decodes and uses the encoded data read from a memory for each memory access using instruction fetch and operand fetch during execution.

[Claim 6] The software accounting method according to claim 1, 2, 3 or 4, wherein when the encoded software is to be decoded and executed,

the user processor secures a region for storing decoded data in advance, and

decodes the whole or partial encoded software at a start of the execution of the software or during the execution and stores the decoded data in the storing region, and

an access given to the region for storing the decoded data is replaced with an access given to a decoding object region during the execution of the software.

[Claim 7] The software accounting method according to claim 1, 2, 3, 4, 5 or 6, wherein the user processor adds the function ID of the software to the software use notice and transmits them to the accounting center, and

the accounting center registers, as registration information, a fourth decoding secret key for decoding a software ID, a function ID corresponding to a function, a rental fee corresponding to a function and the software corresponding to a function for each accounting object software,

retrieves the registration information to acquire the

rental fee for the function and the fourth decoding secret key by using the software ID and the function ID which are transmitted from the user processor, and

retrieves the user information by using the invoicee ID and the rental fee for the function and updates accounting information corresponding to the invoicee ID.

[Claim 8] The software accounting method according to claim 1, wherein when encoding a part of a software to be provided to a user,

the information providing system encodes data within an address range of the software.

[Claim 9] The software accounting method according to claim 1, wherein when encoding a part of a software to be provided to a user,

the information providing system encodes the software in a unit of a function.

[Claim 10] The software accounting method according to claim 1, wherein when encoding a part of a software to be provided to a user,

the information providing system encodes all encoding object regions of the software with one kind of secret key.

[Claim 11] The software accounting method according to claim 10, wherein when encoding a part of a software to be provided to a user,

the information providing system divides the encoding object region of the software into a plurality of subregions and

encodes the subregions thus divided with different secret keys, respectively.

[Claim 12] A software accounting system comprising a user processor using a provided software, an accounting center for carrying out an accounting processing for a software to be used by the user processor, and a network for connecting the user processor and the accounting center, comprising an information providing system having:

first encoding means for encoding the software to be provided to the user processor by using a first decoding secret key; and

software providing means for providing the encoded software to the user processor,

the accounting center having:

accounting means for carrying accounting for the software to be used by the user processor based on a software use notice received from the user processor; and

decoding key transmitting means for transmitting the first decoding secret key used in the first encoding means to the user processor when the accounting processing is ended, and

the user processor having:

ID registering means for registering a self-device ID on the accounting center in advance;

use notifying means for giving the accounting center a software use notice that the distributed software is used; and

first decoding means for decoding and executing a whole or partial encoded region of the software by using the first

decoding secret key received from the accounting center.

[Claim 13] The software accounting system according to claim 12, wherein the accounting means of the accounting center includes:

accounting information storing means for storing a software ID, a rental fee for a software and a first decoding secret key for decoding an encoded software for each accounting object software;

user information storing means for holding an invoicee ID and user accounting information for each user;

first retrieving means for retrieving the accounting information storing means to acquire the rental fee for a software and the first decoding secret key by using the software ID; and

first accounting information updating means for retrieving the user information storing means based on the invoicee ID transmitted through the user notifying means from the user processor to acquire user accounting information corresponding to the invoicee ID and to update the user accounting information with the rental fee for the software.

[Claim 14] The software accounting system according to claim 12 or 13, wherein the notifying means of the user processor includes:

random number generating means for generating a random number; and

random number transmitting means for transmitting the random number generated by the random number generating means

together with the software use notice to the accounting center,

the first decoding means includes random number deciding means for comparing the random number received from the accounting center with the random number generated by the random number generating means and deciding whether or not both of them are coincident with each other, and carrying out decoding only when they are coincident with each other, and

the decoding key transmitting means of the accounting center includes random number transmitting means for transmitting the random number received from the user processor together with the first decoding secret key through the random number transmitting means.

[Claim 15] The software accounting system according to claim 12, 13 or 14, wherein the accounting information storing means of the accounting center further includes a second secret key for encoding the first decoding secret key corresponding to the software,

the decoding key transmitting means includes second encoding means for generating encoded information obtained by encoding the first decoding secret key to be transmitted to the user processor by using the second secret key, and

the first decoding means of the user processor includes second decoding means for extracting the second secret key buried in the software to decode the encoded information received from the accounting center with the second secret key, thereby acquiring the first decoding secret key and decoding the software with the first decoding secret key.

[Claim 16] The software accounting system according to claim 12, 13, 14 or 15, wherein the use notifying means of the user processor further has:

sign generating means for encoding a part of a software use notice to be transmitted to the accounting center by using a private secret key of an invoicee, thereby generating a sign; and

sign transmitting means for transmitting the sign together with the software use notice to the accounting center,

the accounting center further includes a public key corresponding to the third private secret key of the invoicee in the user information storing means, and

user information deciding means for decoding the sign received from the user processor by using the public key for decoding the sign corresponding to the third private secret key of the invoicee on the user information storing means, thereby deciding coincidence with the software use notice received from the user processor.

[Claim 17] The software accounting system according to claim 12, 13, 14, 15 or 16, wherein the first decoding means includes mean for decoding and using encoded data read from a memory every memory access using an instruction fetch and an operand fetch.

[Claim 18] The software accounting system according to claim 12, 13, 14, 15 or 16, wherein the first decoding means includes decoded data storing means for storing predecoded data, and alternate access means for wholly or partially decoding the encoded data and storing the decoded data in the decoded data

storing means at a start of execution of the software or during the execution, and substituting an access given to a decoding object region during the execution of the software for an access given to the decoded data storing means.

[Claim 19] The software accounting system according to claim 12, 13, 14, 15, 16, 17 or 18, wherein the accounting center further has:

second accounting information storing means for storing, for each accounting object software, a software ID, a function ID corresponding to a function, a rental fee corresponding to a function and a fourth decoding secret key transmitted to the user processor for decoding an accounting object software corresponding to a function;

second retrieving means the second accounting information storing means to acquire the rental fee for the function and the fourth decoding secret key by using the software ID and the function ID; and

second accounting information updating means for retrieving the user information storing means to update the user accounting information corresponding to the invoicee ID by using the invoicee ID and the rental fee for the function, and

the user processor further has ID notifying means for transmitting the function ID together with the invoicee ID and the software ID to the accounting center.

[Claim 20] The software accounting system according to claim 12, wherein the first encoding means of the information providing system includes means for encoding data within an

address range of the software.

[Claim 21] The software accounting system according to claim 12, wherein the first encoding means of the information providing system includes means for encoding data in a unit of a function of the software.

[Claim 22] The software accounting system according to claim 12, wherein the first encoding means of the information providing system includes means for encoding all encoding object regions of the software with one kind of secret key.

[Claim 23] The software accounting system according to claim 22, wherein the first encoding means of the information providing system includes means for dividing the encoding object region of the software into a plurality of subregions and encoding the divided subregions with different secret keys when encoding a part of the software provided to the user processor.

[Detailed Description of the Invention]

[0001]

[Technical Field of the Invention] The present invention relates to a software accounting method and system, and more particularly to a software accounting method and system for carrying out accounting for a software stored in a medium such as a CD-ROM or a floppy disk and distributed or a software distributed through a network.

[0002]

[Prior Art] Examples of a conventional software accounting system include a method of selling a software and ending

accounting when a user purchases the software. Moreover, there has been a system for notifying an accounting center that a user will utilize the distributed software so that the accounting center carries out accounting for the use of the software.

[0003] Recently, there has also been employed a method of distributing a software encoded as a variant of a purchasing form through a medium such as a CD-ROM or a network and performing a procedure for purchase through a telephone, a facsimile, a letter or an electronic mail and then giving a decryption key. Furthermore, there has been a method of distributing an encoded software having the amount of availability set in advance, managing the amount of a user's utilization through the number of days and carrying out accounting based on the number of days.

[0004]

[Problems to be Solved] In the above-mentioned purchasing methods, however, a circulation cost is relatively reduced so that the function of the software is enlarged and the user should bear a great expense including the functions which are rarely used. Moreover, it is necessary to purchase and execute a software in order to decide whether or not the function required by the user is satisfied.

[0005] In the method of simply notifying the accounting center that the user will utilize the distributed software, moreover, the accounting can be carried out but the use of the software cannot be restricted. Therefore, there has been a

problem in that countermeasures cannot be taken even if the fee for use has not been paid.

[0006] Also in the system in which the encoded software is provided in advance and the decryption key is provided during use, the user should pay the same amount of money irrespective of the number of times of the use and the number of times of the use or a price per using time has a great range. In consideration of the above-mentioned respects, it is an object of the present invention to provide a software accounting method and system capable of collecting the amount of use proportional to the number of times of the use corresponding to the function of using a software.

[0007] More specifically, it is an object to provide a software accounting method and system in which user accounting information is updated for the requirement of use of the software, and the permission of use is then given, it is guaranteed that the software permitted to be used can be utilized only once and a fee per use can be reduced.

[0008]

[Solution to the Problems] Fig. 1 is a diagram showing the principle of the present invention. The present invention provides a software accounting method for accounting a rental fee for a software to be provided to a user processor, wherein an information providing system encodes a whole or partial software to be provided to an invoicee and distributes the software thus encoded to a user (Step 1), an accounting center registers, as registration information, a software identifier,

a rental fee for the software and a first decoding secret key for decoding the encoded software for each accounting object software (Step 2), the invoicee registers an invoicee ID to the accounting center (Step 3), when the invoicee activates the software (Step 4) and transmits a software use notice including the software ID to the accounting center (Step 5), the accounting center retrieves the rental fee for the software and the first decoding secret key based on the software use notice (Step 6), updates accounting information corresponding to the invoicee ID with the rental fee for the software (Step 7), and transmits the first decoding secret key thus acquired to the user processor (Step 8), and the user processor decodes (Step 9) and executes (Step 10) the whole or partial encoded region of the software by using the first decoding secret key received from the accounting center.

[0009] In the present invention, moreover, the user processor generates a random number and transmits the random number together with the software use notice to the accounting center, the accounting center receives the random number from the user processor and transmits the received random number together with the first decoding secret key to the user processor, and the user processor receives the first decoding secret key and the random number from the accounting center, and compares the generated random number with the received random number and decides whether they are coincident with each other or not, and decodes the software only when they are coincident with each other.

[0010] In the present invention, furthermore, the accounting center further includes, as the registration information, a second secret key for encoding the first decoding secret key corresponding to the software, and transmits encoded information to be the encoded first decoding secret key to the user processor by using the second secret key, and the user processor extracts the second secret key buried in the software, decodes the encoded information to acquire the first decoding secret key by using the second secret key, and decodes the software by using the first decoding secret key thus acquired.

[0011] In the present invention, moreover, the user processor encodes a part of information to be transmitted to the accounting center by using a third private secret key of an invoicee, thereby generating a sign to be transmitted to the accounting center, and the accounting center further includes a public key corresponding to a third private secret key of the invoicee and decides whether or not information obtained by decoding the sign with the public key is coincident with other information received from the user processor, and transmits the first decoding secret key to the user processor only when they are coincident with each other.

[0012] In the present invention, furthermore, the user processor decodes the encoded software and decodes and uses the encoded data read from a memory for each memory access using instruction fetch and operand fetch during execution.

[0013] In the present invention, moreover, when the encoded software is to be decoded and executed, the user

processor secures a region for storing decoded data in advance, and decodes the whole or partial encoded software at a start of the execution of the software or during the execution and stores the decoded data in the storing region, and an access given to the region for storing the decoded data is replaced with an access given to a decoding object region during the execution of the software.

[0014] In the present invention, furthermore, the user processor adds the function ID of the software to the software use notice and transmits them to the accounting center, and the accounting center registers, as registration information, a fourth decoding secret key for decoding a software ID, a function ID corresponding to a function, a rental fee corresponding to a function and the software corresponding to a function for each accounting object software, retrieves the registration information to acquire the rental fee for the function and the fourth decoding secret key by using the software ID and the function ID which are transmitted from the user processor, and retrieves the user information by using the invoicee ID and the rental fee for the function and updates accounting information corresponding to the invoicee ID.

[0015] In the present invention, moreover, when encoding a part of a software to be provided to a user, the information providing system encodes data within an address range of the software. In the present invention, furthermore, when encoding a part of a software to be provided to a user, the information providing system encodes the software in a unit of

a function.

[0016] In the present invention, moreover, when encoding a part of a software to be provided to a user, the information providing system encodes all encoding object regions of the software with one kind of secret key. In the present invention, furthermore, when encoding a part of a software to be provided to a user, the information providing system divides the encoding object region of the software into a plurality of subregions and encodes the subregions thus divided with different secret keys, respectively.

[0017] Fig. 2 is a diagrams showing the structure of the principle of the present invention. The present invention provides a software accounting system comprising a user processor 100 using a provided software, an accounting center 200 for carrying out an accounting processing for a software to be used by the user processor 100, and a network for connecting the user processor 100 and the accounting center 200, comprising an information providing system having first encoding means for encoding the software to be provided to the user processor 100 by using a first decoding secret key, and software providing means for providing the encoded software to the user processor 100, the accounting center 200 having accounting means 240 for carrying accounting for the software to be used by the user processor 100 based on a software use notice received from the user processor 100, and decoding key transmitting means 250 for transmitting the first decoding secret key used in the first encoding means to the user processor 100 when the accounting

processing is ended, and the user processor 100 having ID registering means 101 for registering a self-device ID on the accounting center 200 in advance, use notifying means 120 for giving the accounting center 200 a software use notice that the distributed software is used, and first decoding means 130 for decoding and executing a whole or partial encoded region of the software by using the first decoding secret key received from the accounting center 200.

[0018] In the present invention, moreover, the accounting means 240 of the accounting center 200 includes accounting information storing means for storing a software ID, a rental fee for a software and a first decoding secret key for decoding an encoded software for each accounting object software, user information storing means for holding an invoicee ID and user accounting information for each user, first retrieving means for retrieving the accounting information storing means to acquire the rental fee for a software and the first decoding secret key by using the software ID, and first accounting information updating means for retrieving the user information storing means based on the invoicee ID transmitted through the user notifying means 120 from the user processor 100 to acquire user accounting information corresponding to the invoicee ID and to update the user accounting information with the rental fee for the software.

[0019] In the present invention, furthermore, the notifying means of the user processor 100 includes random number generating means for generating a random number, and random

number transmitting means for transmitting the random number generated by the random number generating means together with the software use notice to the accounting center 200, the first decoding means 130 includes random number deciding means for comparing the random number received from the accounting center 200 with the random number generated by the random number generating means and deciding whether or not both of them are coincident with each other, and carrying out decoding only when they are coincident with each other, and the decoding key transmitting means 250 of the accounting center 200 includes random number transmitting means for transmitting the random number received from the user processor 100 together with the first decoding secret key through the random number transmitting means.

[0020] In the present invention, moreover, the accounting information storing means of the accounting center 200 further includes a second secret key for encoding the first decoding secret key corresponding to the software, the decoding key transmitting means 250 includes second encoding means for generating encoded information obtained by encoding the first decoding secret key to be transmitted to the user processor 100 by using the second secret key, and the first decoding means 130 of the user processor 100 includes second decoding means for extracting the second secret key buried in the software to decode the encoded information received from the accounting center 200 with the second secret key, thereby acquiring the first decoding secret key and decoding the software with the

first decoding secret key.

[0021] In the present invention, furthermore, the use notifying means 120 of the user processor 100 further has sign generating means for encoding a part of a software use notice to be transmitted to the accounting center 200 by using a private secret key of an invoicee, thereby generating a sign, and sign transmitting means for transmitting the sign together with the software use notice to the accounting center 200, the accounting center 200 further includes a public key corresponding to the third private secret key of the invoicee in the user information storing means, and user information deciding means for decoding the sign received from the user processor 100 by using the public key for decoding the sign corresponding to the third private secret key of the invoicee on the user information storing means, thereby deciding coincidence with the software use notice received from the user processor 100.

[0022] In the present invention, moreover, the first decoding means includes mean for decoding and using encoded data read from a memory every memory access using an instruction fetch and an operand fetch. In the present invention, furthermore, the first decoding means includes decoded data storing means for storing predecoded data, and alternate access means for wholly or partially decoding the encoded data and storing the decoded data in the decoded data storing means at a start of execution of the software or during the execution, and substituting an access given to a decoding object region during the execution of the software for an access given to the

decoded data storing means.

[0023] In the present invention, moreover, the accounting center storing, for each accounting object software, a software ID, a function ID corresponding to a function, a rental fee corresponding to a function and a fourth decoding secret key transmitted to the user processor 100 for decoding an accounting object software corresponding to a function, second retrieving means the second accounting information storing means to acquire the rental fee for the function and the fourth decoding secret key by using the software ID and the function ID, and second accounting information updating means for retrieving the user information storing means to update the user accounting information corresponding to the invoicee ID by using the invoicee ID and the rental fee for the function, and the user processor 100 further has ID notifying means for transmitting the function ID together with the invoicee ID and the software ID to the accounting center 200.

[0024] In the present invention, furthermore, the first encoding means of the information providing system includes means for encoding data within an address range of the software. In the present invention, moreover, the first encoding means of the information providing system includes means for encoding data in a unit of a function of the software.

[0025] In the present invention, moreover, the first encoding means of the information providing system includes means for encoding all encoding object regions of the software with one kind of secret key. In the present invention,

furthermore, the first encoding means of the information providing system includes means for dividing the encoding object region of the software into a plurality of subregions and encoding the divided subregions with different secret keys when encoding a part of the software provided to the user processor 100.

[0026] In the above-mentioned invention, it is assumed that the whole or partial software to be provided to the user is encoded in advance during the development of the software or before provision. In the case in which a part of the software is to be encoded, data may be encoded in a certain address range, an instruction section or a data section may be encoded, or the encoding may be carried out in a unit of a function. Moreover, all the encoding object regions may be encoded with one kind of secret key or the encoding object regions may be divided into a plurality of subregions to be encoded with different secret keys. Thus, the encoding can be carried out by various methods.

[0027] In the present invention, moreover, the softw3are ID, the rental fee for the software and the secret key for decoding the encoded software are registered in the accounting information storing means of the accounting center before providing the software. Furthermore, the user registers the invoicee ID on the user information table of the accounting center prior to the use of the software.

[0028] When the user activates the software on the user processor and transmits the software ID and the invoicee ID from the user processor to the accounting center before the execution

of the software or the execution, the accounting center retrieves the accounting information storing means by using the software ID received from the user processor and acquires the rental fee for the software and the secret key for the decoding. Next, the user information storing means is retrieved by using the invoicee ID received from the user processor and the user accounting information of the invoicee is updated by using the rental fee for the software acquired from the accounting information table. Thus, the accounting processing for each invoicee is carried out. Furthermore, the accounting center transmits, to the user processor, the secret key for the decoding which is acquired from the accounting information storing means. Consequently, the user processor decoded and executes the whole or partial encoded region of the software by using the secret key received from the accounting center.

[0029] Consequently, when the encoded software is to be provided from the information providing system and the user is to execute (activate) the software, the accounting processing is carried out in the accounting center to transmit the secret key for using the software. Thus, the user can be permitted to use the software.

[0030] Furthermore, a part of the software is encoded and transmitted. Consequently, in the case in which the user does not utilize any software, he (or she) does not pay for the unused software. In the present invention, moreover, the random number generated by the user processor is transmitted to the accounting center and is checked with the random number returned

from the accounting center. Only when they are coincident with each other, the software is decoded. Thus, it is possible to prevent a third party from irregularly use the software.

[0031] In the present invention, moreover, the encoded information obtained by further encoding the first decoding secret key for decoding the software is transmitted to the user processor, and the user processor decodes and executes the software by using the first decoding key acquired by decoding the encoded information. Consequently, the user cannot decode the software as long as the encoded information received from the accounting center cannot be decoded.

[0032] In the present invention, furthermore, the sign is generated in the user processor and is transmitted to the accounting center. In the accounting center, it is decided whether or not information obtained by decoding the sign is coincident with other information which is received. IF they are not coincident with each other, the first decoding secret key is not transmitted to the user processor. Therefore, in the case in which a malicious third party transmits another sign, the software cannot be decoded and executed.

[0033] In the present invention, moreover, the region for storing the decoded data is set so that the decoded software is sequentially stored in the region. Consequently, the software is accessed in the region during the execution. Thus, efficient access can be given because the decoded software is stored.

[0034] In the present invention, furthermore, the

function ID of the software is transmitted together with the software ID and the invoicee ID from the user processor to the accounting center. Consequently, it is possible to carry out the accounting in a unit of a function group in the software to be activated.

[0035]

[Preferred Embodiments of the Invention] Fig. 3 is a diagram showing the structure of a system according to the present invention. The system which will be described below is constituted by a user processor 100, an accounting center 200, and a communication network (not shown) for connecting the user processor 100 and the accounting center 200.

[0036] The accounting center 200 is an information provider for providing a software and serves to execute an accounting system, which will be hereinafter referred to as an accounting center for convenience. The information provider and the accounting center may be set separately and independently. The user processor 100 has an accounting center transmitting section 120 and a decoding section 130. The decoding section 130 serves to decode a software 110 to be accounted by using a decryption key (which will be hereinafter referred to as a first decoding and secret key). The software 110 is encoded wholly or partially by using one or more secret keys, and is provided from the accounting center 200 (information provider) in advance.

[0037] The accounting center transmitting section 120 serves to transmit user information such as an invoicee ID of

a device itself and a software ID to be activated. The accounting center 200 has an accounting information table 210, a user information table 220, an accounting information table retrieving section 230, a user accounting information updating section 240, and a user processor transmitting section 250.

[0038] The accounting information table 210 is constituted by a software ID, a software rental fee, and a first decoded secret key for decoding the encoded software. In the following description, it is assumed that a software to be distributed to the user processor 100 is wholly or partially encoded and transmitted to the user processor 100 and a secret key used during the encoding is set to be the first decoded secret key and is registered in the accounting information table 210 of the accounting center 200.

[0039] The user information table 220 is constituted by the recipient transferred from the user processor 100 and the user accounting information. The accounting information table retrieving section 230 retrieves the accounting information table 210 by using the software ID received from the user processor 100, acquires and transfers the rental fee of the software to the user accounting information updating section 240, and furthermore, acquires and transfers the first decoded secret key to the user processor transmitting section 250.

[0040] The user accounting information updating section 240 retrieves the user information table 220 by using the invoicee ID received from the user processor 100, acquires the user accounting information of the invoicee and update the user

accounting information with the rental fee of the software. The user processor transmitting section 250 transfers, to the user processor 100, the first decoded secret key acquired from the accounting information table retrieving section 230.

[0041]

[Embodiment] Preferred embodiments of the present invention will be described below in detail with reference to the drawings.

[First Embodiment] A system structure according to the present embodiment is shown in Fig. 3 described above.

[0042] Fig. 4 is a diagram illustrating an operation according to a first embodiment of the present invention.

Step 101) A user processor 100 activates a software 110 provided from an information provider in advance.

Step 102) The software 110 is loaded onto a memory.

[0043] Step 103) When the encoded software 110 is activated in the user processor 100, an accounting center transmitting section 120 of the user processor 100 transmits a software ID and an invoicee ID to an accounting center 200.

Step 104) The accounting center 200 receives the software ID and the invoicee ID from the user processor 100, and the accounting information table retrieving section 230 retrieves the accounting information table 210 by using the software ID, and acquires the rental fee for a software corresponding to the software ID and a first decoded secret key.

[0044] Step 105) A user accounting information updating section 240 retrieves the user information table 220

by using the received invoicee ID, acquires the user accounting information about the invoicee, and updates the user accounting information by using the rental fee for a software retrieved by the accounting information table retrieving section 230 (the rental fee for the software is added to the user accounting information).

[0045] Step 106) A user processor transmitting section 250 transmits the first decoded secret key retrieved by the accounting information table retrieving section 230 to the user processor 100.

Step 107) The user processor 100 decodes and executes the whole or partial encoded region of the software by using the first decoded secret key received from the accounting center 200.

[0046] According to the present embodiment, thus, the software ID and the invoicee ID are transmitted as a software use notice from the user processor 100 to the accounting center 200. Consequently, the first decoding and secret key for decoding the software can be received from the accounting center and the encoded software can be decoded and executed.

[0047]

[Second Embodiment] In the present embodiment, a processing of deciding whether or not the permission for decoding a software can be carried out by using a random number is added to the first embodiment described above. Fig. 5 is a diagram showing the structure of a system according to a second embodiment of the present invention. In Fig. 5, the same

components as those in Fig. 3 have the same reference numerals and description will be omitted.

[0048] With the structure shown in Fig. 5, a user processor 100 comprises a random number generating section 140 for generating a random number and a comparing section 150, and an accounting center 200 comprises a random number receiving section 260 in the structure of the system shown in Fig. 3. The random number generating section 140 of the user processor 100 generates a random number, transfers the random number to the accounting center transmitting center 120, and transmits the random number from the accounting center transmitting section 120 to the accounting center 200. The comparing section 150 compares a random number returned from the accounting center 200 with a random number generated from the random number generating section 140 and a random number returned from the accounting center 200. If they are coincident with each other, the decoding section 120 is permitted to decode the software 100.

[0049] The random number receiving section 260 of the accounting center 200 carries out a processing of returning the random number acquired from the user processor 100 to the user processor 100 through a user processor transmitting section 250.

[0050] Fig. 6 is a diagram illustrating an operation according to the second embodiment of the present invention. Step 201) A user processor 100 activates a software 110 provided from an information provider in advance.

Step 202) The software 110 is loaded onto a memory.

[0051] Step 203) The random number generating section 140 generates a random number and transfers the random number to the accounting center transmitting section 120.

Step 204) The accounting center transmitting section 120 transmits the software ID, the invoicee ID and the random number to the accounting center 200.

[0052] Step 205) In the accounting center 20, the random number receiving section 260 receives the random number, and receives the software ID and the invoicee ID from the user processor 100, the accounting information table retrieving section 230 retrieves an accounting information table 210 by using the software ID, and acquires a rental fee for the software corresponding to the software ID and a first decoded secret key in the same manner as in the first embodiment.

[0053] Step 206) A user accounting information updating section 240 retrieves the user information table 220 by using the received invoicee ID, acquires the user accounting information about the invoicee, and updates the user accounting information by using the rental fee for a software retrieved by the accounting information table retrieving section 230 (the rental fee for the software is added to the user accounting information).

[0054] Step 207) A user processor transmitting section 250 transmits the first decoded secret key retrieved by the accounting information table retrieving section 230 and the random number received by the random number receiving section

260 to the user processor 100.

Step 208) The user processor 100 compares the random number received by the accounting center 200 with the random number generated at the Step 203. If they are coincident with each other, the decoding section 130 decodes and executes the whole or partial encoded region of the software by using the first decoded secret key received from the accounting center 200.

[0055] In the present embodiment, only when the random number transmitted from the user processor 100 to the accounting center 200 is coincident with the random number received from the accounting center 200, the software can be decoded.

[Third Embodiment] The structure of a system according to the present embodiment is basically identical to the structure shown in Fig. 3 except that an accounting information table 210 holds a second secret key, an accounting information retrieving section 230 retrieves the second secret key based on a software ID, and a user accounting information updating section 240 encodes a first decoded secret key.

[0056] Fig. 7 is a diagram illustrating an operation according to a third embodiment of the present invention.

Step 301) A user processor 100 activates a software 110 provided from an information provider in advance.

Step 302) The software 110 is loaded onto a memory.

[0057] Step 303) An accounting center transmitting section 120 transmits a software ID and an invoicee ID to an accounting center 200.

Step 304) The accounting center 200 receives the software ID

and the invoicee ID from the user processor 100, and the accounting information table retrieving section 230 retrieves the accounting information table 210 by using the software ID, and acquires the rental fee for a software corresponding to the software ID, a first decoded secret key and a second secret key.

[0058] Step 305) A user accounting information updating section 240 retrieves the user information table 220 by using the received invoicee ID, acquires the user accounting information about the invoicee, and updates the user accounting information by using the rental fee for a software retrieved by the accounting information table retrieving section 230 (the rental fee for the software is added to the user accounting information).

[0059] Step 306) Furthermore, a user accounting information updating section 240 encodes the first decoded secret key by using the second secret key acquired from the accounting information table 210 and transfers the first decoded secret key thus encoded to a user processor transmitting section 250.

Step 307) The user processor transmitting section 250 transmits, to the user processor 100, the information encoded by the user accounting information updating section 240.

[0060] Step 308) The decoding section 130 of the user processor 100 decodes the encoded information received from the accounting center 200 by using the second secret key buried in the software 110 and thus acquires the first decoded secret

key.

Step 309) Furthermore, the decoding section 130 decodes and executes the whole or partial encoded region of the software by using the first decoded secret key acquired by the decoding at the Step 308.

[0061] According to the present embodiment, thus, the first decoded secret key is encoded and transmitted to the user processor. Consequently, it is possible to transmit a safer first decoded secret key.

[Fourth Embodiment] Fig. 8 is a diagram showing the structure of a system according to a fourth embodiment of the present invention. In Fig. 8, the same components as those in Fig. 3 have the same reference numerals and description will be omitted.

[0062] The structure of a system shown in Fig. 8 is different from that shown in Fig. 3 in that a user processor 100 comprises a third private secret key holding section 160 and a sign generating section 170. The third private secret key holding section 160 holds a third private secret key for generating a sign. The sign generating section 170 generates a sign by using the third private secret key.

[0063] Moreover, a user information table 220 of an accounting center 200 holds a public key for decoding a sign in addition to an invoicee ID and accounting information. Fig. 9 is a diagram showing the detailed structure of a user accounting information updating section according to a fourth embodiment of the present invention. The user accounting

information updating section 240 shown in Fig. 9 includes a table retrieving section 241 for retrieving a user information table and acquiring a public key, a sign decoding section 242 for decoding the sign acquired from the user processor 100 by using the public key, a comparing section 243 for comparing other information received from the user processor 100 with the decoded information, and a table updating section 244 for updating a user information table 220.

[0064] As long as the decoded information is coincident with the information received from the user processor 100 in the comparing section 243, the table updating section 244 updates the user accounting information of an invoicee with a rental fee for a software which is acquired from an accounting information table retrieving section 230, and furthermore, transfers a first decoded secret key acquired from the table retrieving section 241 to a user processor transmitting section 250.

[0065] Fig. 10 is a diagram illustrating an operation according to the fourth embodiment of the present invention.

Step 401) A user processor 100 activates a software 110 provided from an information provider in advance.

Step 402) The software 110 is loaded onto a memory.

[0066] Step 403) The sign generating section 170 of the user processor 100 reads a third private secret key from the third private secret key holding section 160 and encodes a part of a software ID and an invoicee ID by using the third private secret key, thereby generating a sign to be transferred to an

accounting center transmitting section 120.

[0067] Step 404) An accounting center transmitting section 120 transmits the encoded software ID and an invoicee ID to an accounting center 200.

Step 405) The table retrieving section 241 of the user accounting information updating section 240 retrieves the user information table 220 for the encoded information thus received and acquires a public key to be transferred to the sign decoding section 242. The sign decoding section 242 acquires the public key of the invoicee, decodes the encoded information by using the public key and transfers the decoded information to the comparing section 243. The comparing section 243 compares the decoded information with other information received from the user processor 100 and decides whether they are coincident with each other. If they are coincident with each other, the processing proceeds to the next step.

[0068] Step 406) The accounting information table retrieving section 230 of the accounting center 200 retrieves the accounting information table 210 by using the software ID and the invoicee ID which are received from the user processor 100, and acquires the rental fee for a software corresponding to the software ID and a first decoded secret key.

[0069] Step 407) The table updating section 244 of the user accounting information updating section 240 acquires the user accounting information from the accounting information table retrieving section 230, and updates the user accounting information by using the rental fee for a software retrieved

by the accounting information table retrieving section 230 (the rental fee for the software is added to the user accounting information).

[0070] Step 408) Furthermore, the user accounting information updating section 240 transfers the first decoded secret key to a user processor transmitting section 250. The user processor transmitting section 250 transmits, to the user processor 100, the information encoded by the user accounting information updating section 240.

[0071] Step 409) The decoding section 130 of the user processor 100 decodes and executes the whole or partial encoded region of the software by using the first decoded secret key. The present invention can also be executed in combination with each of the above-mentioned embodiments. Consequently, if the information is not coincident with the sign, the first decoded secret key is not transmitted from the accounting center 200 to the user processor 100. Therefore, the user should have a proper sign in order to decode the software.

[0072]

[Fifth Embodiment] The structure of a system according to the present embodiment is basically identical to that shown in Fig. 3. Fig. 11 is a diagram illustrating an operation according to a fifth embodiment of the present invention.

Step 501) In a user processor 100, a software 110 having an instruction portion encoded in advance is activated.

[0073] Step 502) The user processor 100 loads the software 100.

Step 503) An accounting center transmitting section 120 of the user processor 100 transmits a software ID and an invoicee ID to an accounting center 200.

[0074] Step 504) An accounting information table retrieving section 230 of the accounting center 200 retrieves an accounting information table 210 by using the software ID received from the user processor 100 and acquires a rental fee for the software and a first decoded secret key.

Step 505) A user accounting information updating section 240 retrieves a user information table 220 by using the invoicee ID received from the user processor 100, and updates the user accounting information of the invoicee with the rental fee for the software acquired from the accounting information table 210.

[0075] Step 506) A user processor transmitting section 250 transmits the first decoded secret key acquired fro the accounting information table retrieving section 230 to the user processor 100.

Step 507) A decoding section 130 of the user processor 100 reads an instruction to be executed next by using the first decoded secret key received from the accounting center 200.

[0076] Step 508) The decoding section 130 decodes the read instruction.

Step 509) The instruction decoded by the decoding section 130 is executed.

The processings of the Steps 508 and 509 are repeated until all the instructions thus decoded are completed.

[0077]

[Sixth Embodiment] Fig. 12 shows the structure of a user processor according to a sixth embodiment of the present invention. In Fig. 12, the same components as those in Fig. 3 have the same reference numerals and description will be omitted. In the present embodiment, the structure is the same as that in Fig. 3.

[0078] In Fig. 12, a user processor 100 comprises a decoded software storing section 180 for storing an instruction decoded by a decoding section 130 and an executing section 190 for sequentially reading and executing the instruction stored in the decoded software storing section 180 in addition to the structure shown in Fig. 3.

[0079] Fig. 13 is a diagram illustrating an operation according to the sixth embodiment of the present invention.

Step 601) In a user processor 100, a software 110 having an instruction portion encoded in advance is activated.

Step 602) The user processor 100 loads the software 100.

[0080] Step 603) An accounting center transmitting section 120 of the user processor 100 transmits a software ID and an invoicee ID to an accounting center 200.

Step 604) An accounting information table retrieving section 230 of the accounting center 200 retrieves an accounting information table 210 by using the software ID received from the user processor 100 and acquires a rental fee for the software and a first decoded secret key.

[0081] Step 605) A user accounting information updating

section 240 retrieves a user information table 220 by using the invoicee ID received from the user processor 100, and updates the user accounting information of the invoicee with the rental fee for the software acquired from the accounting information table 210.

[0082] Step 606) A user processor transmitting section 250 transmits the first decoded secret key acquired fro the accounting information table retrieving section 230 to the user processor 100.

Step 607) A decoding section 130 of the user processor 100 decodes a whole or partial encoded region of the software by using the first decoded secret key received from the accounting center 200.

[0083] Step 608) The decoding section 130 stores the decoded software in the decoded software storing section 180.

Step 609) The executing section 190 accesses the decoded software storing section 1890 and executes the decoded software.

[0084]

[Seventh Embodiment] An accounting information table 210 according to the present embodiment includes a software ID, a function ID corresponding to a function, the amount of use corresponding to a function, and a fourth decoding secret key for decoding as the whole or partial region of an encoded software corresponding to a function. The fourth encoding secret key is transmitted to the user processor 100 and serves to decode a software 110.

[0085] Fig. 14 is a diagram illustrating an operation according to a seventh embodiment of the present invention.

Step 701) A user processor 100 activates a software encoded by using a different secret key for each function in advance.

Step 702) The activated software is loaded onto a memory.

[0086] Step 703) An accounting center transmitting section 120 of the user processor 100 transmits a function ID (function A) of a function to be executed, a software ID and an invoicee ID to an accounting center 200.

Step 704) An accounting information table retrieving section 230 of the accounting center 200 retrieves an accounting information table 210 by using the software ID and the function ID which are received from the user processor, and acquires a rental fee for the function and a fourth decoding secret key.

[0087] Step 705) A user accounting information updating section 240 updates a user information table 220 with the rental fee for the function acquired by the accounting information table retrieving section 230.

Step 706) A user processor transmitting section 250 transmits a first decoding secret key acquired from the accounting information table 210 to the user processor 100.

[0088] Step 707) The user processor 100 decodes and executes the wholly or partial encoded region of the software of the function by using the first decoding secret key received from the accounting center 200. The above-mentioned procedure is repeated in a unit of a function unit by using the software until a processing required by a user is ended. At and after

Step 708,a "function B" is transmitted as a function ID from the user processor 100 to the accounting center 200, and the same processings as the Steps 704 to 707 are repeated.

[0089] In each of the above-mentioned embodiments, the user accounting information can be applied to any of a prepayment method, a postpayment method, a cumulative accounting method, a detail accounting method and a credit payment method. Moreover, while the software has been described as a program in each of the above-mentioned embodiments, it is not restricted but the present invention can be applied to all digital information including voice information, video information, image information and text information in addition to the program.

[0090] The present invention is not restricted to the above-mentioned embodiments but can be variously changed and applied without departing from the scope of the invention.

[0091]

[Effects of the Invention] As described above, according to the soft accounting method and system of the present invention, the software which does not include the encoded portion is not present at any point on a storage medium such as a memory or a disk. Therefore, it is possible to surely prevent the repetitive use of the software. Every time the software is used, the rental fee can surely be collected. Consequently, the user can utilize only a necessary function with a small rental fee.

[0092] By selecting the number of secret keys to be used for encoding a software and the range for the encoding, the

accounting can be carried out in a unit of the software to be activated, and furthermore, the accounting can be carried out in a unit of a function group in the software to be activated. Moreover, it is possible to prevent the collecting leakage of the rental fee by registering prepayment of the rental fee or a credit based on a minimum rental fee and managing the balance of the rental fee.

[0093] Moreover, by verifying whether or not the random number attached for transmission from the user processor to the accounting center is coincident with the random number attached for transmission from the accounting center to the user processor, it is possible to prevent the irregular use of the software due to snatching of the information transmitted from the accounting center to the user processor.

[0094] In the transmission from the accounting center to the user processor, moreover, the public encoding method is used to attach a sign. Consequently, it is possible to prevent the irregular use of the software using another invoicee ID.

[Brief Description of the Drawings]

[Fig. 1] A diagram illustrating the principle of the present invention.

[Fig. 2] A diagram showing the structure of the principle of the present invention.

[Fig. 3] A diagram showing the structure of a system according to the present invention.

[Fig. 4] A diagram illustrating an operation according to a first embodiment of the present invention.

[Fig. 5] A diagram showing the structure of a system according to a second embodiment of the present invention.

[Fig. 6] A diagram illustrating an operation according to the second embodiment of the present invention.

[Fig. 7] A diagram illustrating an operation according to a third embodiment of the present invention.

[Fig. 8] A diagram showing the structure of a system according to a fourth embodiment of the present invention.

[Fig. 9] A diagram showing the structure of a user accounting information updating section according to the fourth embodiment of the present invention.

[Fig. 10] A diagram illustrating an operation according to the fourth embodiment of the present invention.

[Fig. 11] A diagram illustrating an operation according to a fifth embodiment of the present invention.

[Fig. 12] A diagram showing the structure of a user processor according to a sixth embodiment of the present invention.

[Fig. 13] A diagram illustrating an operation according to the sixth embodiment of the present invention.

[Fig. 14] A diagram illustrating an operation according to a seventh embodiment of the present invention.

[Designation of the Reference Numerals]

100 user processor

101 ID registering means

110 software

120 accounting center transmitting section, use notifying means

130 decoding section, first decoding and secret means

140 random number generating section

150 comparing section

160 third secret key holding section

170 sign generating section

180 decoded software storing section

190 executing section

200 accounting center

201 first encoding means

202 software providing means

210 accounting information table

220 user information table

230 accounting information table retrieving section

240 user accounting information updating section, accounting means

241 table retrieving section

242 sign decoding means

243 comparing section

244 table updating section

250 user processor transmitting section, decryption key transmitting means

260 random number receiving section

FIG. 1.
Diagram illustrating principle of the present invention

【図１】

本発明の原理を説明するための図

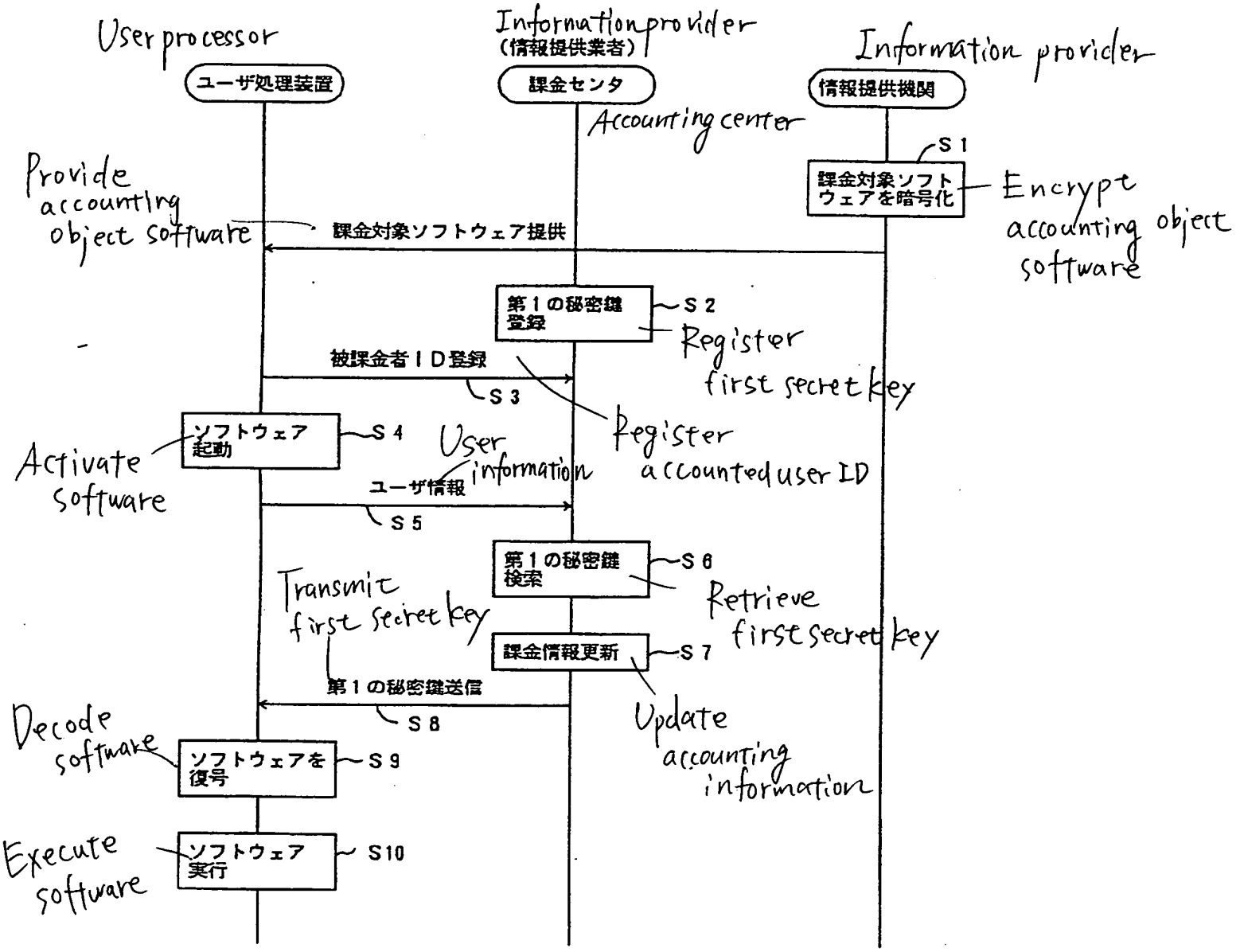


FIG. 2

Diagram illustrating structure of principle of the present invention

【図２】

本発明の原理構成図

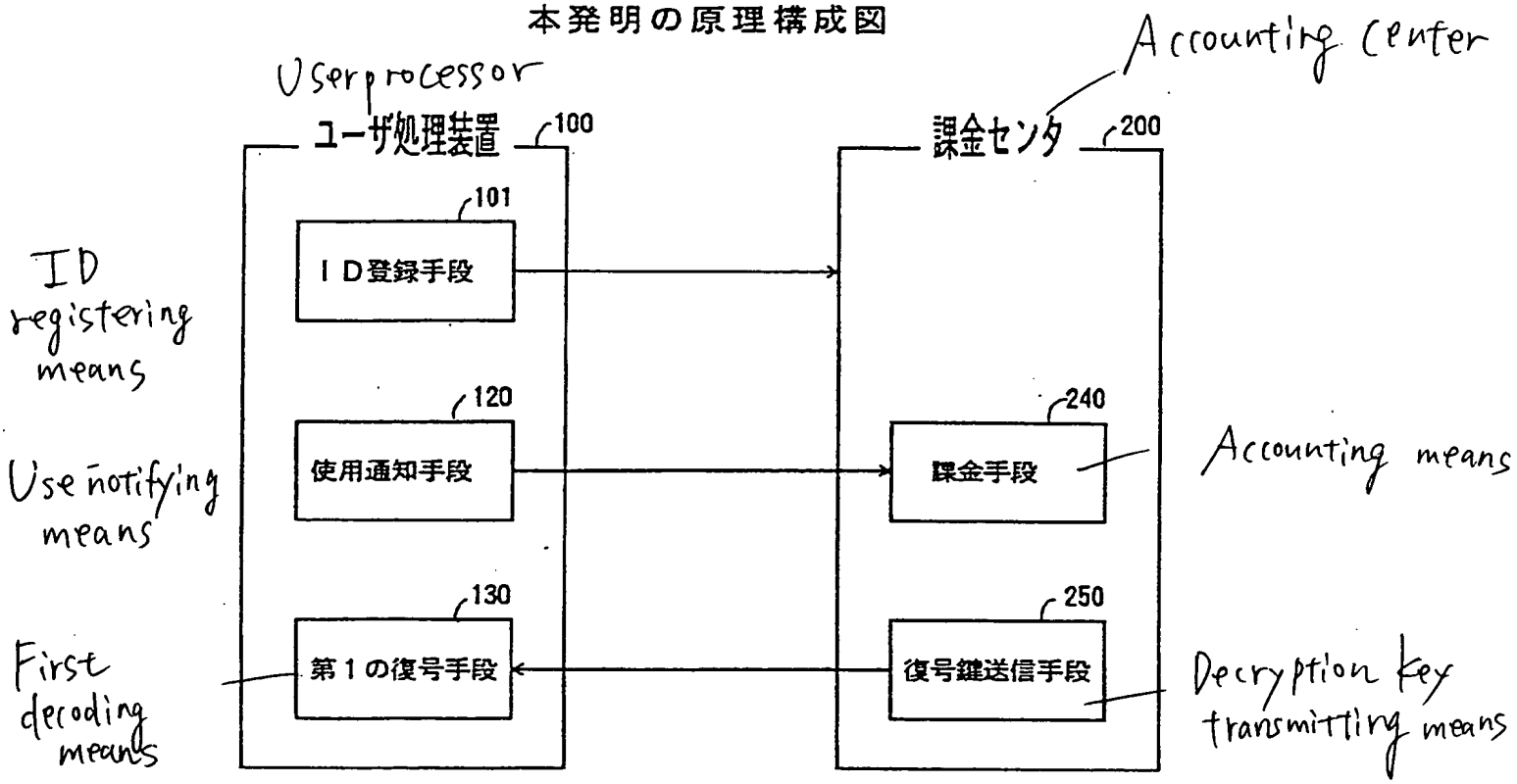


FIG. 3.
Diagram illustrating structure of system according to the present invention

【図３】

本発明のシステム構成図

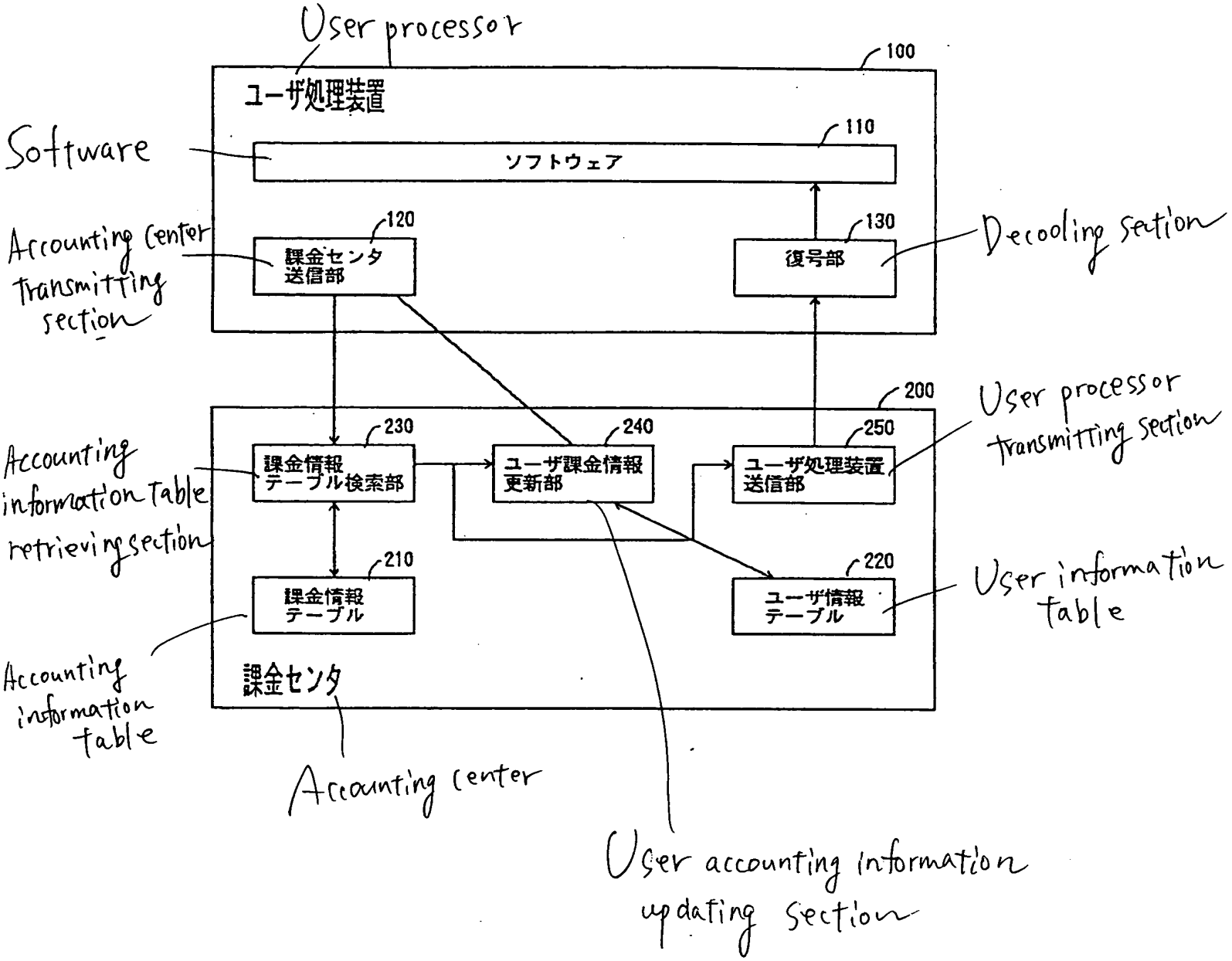


FIG. 4
Diagram illustrating operation according to first embodiment of the present invention

【図４】

本発明の第１の実施例の動作を説明するための図

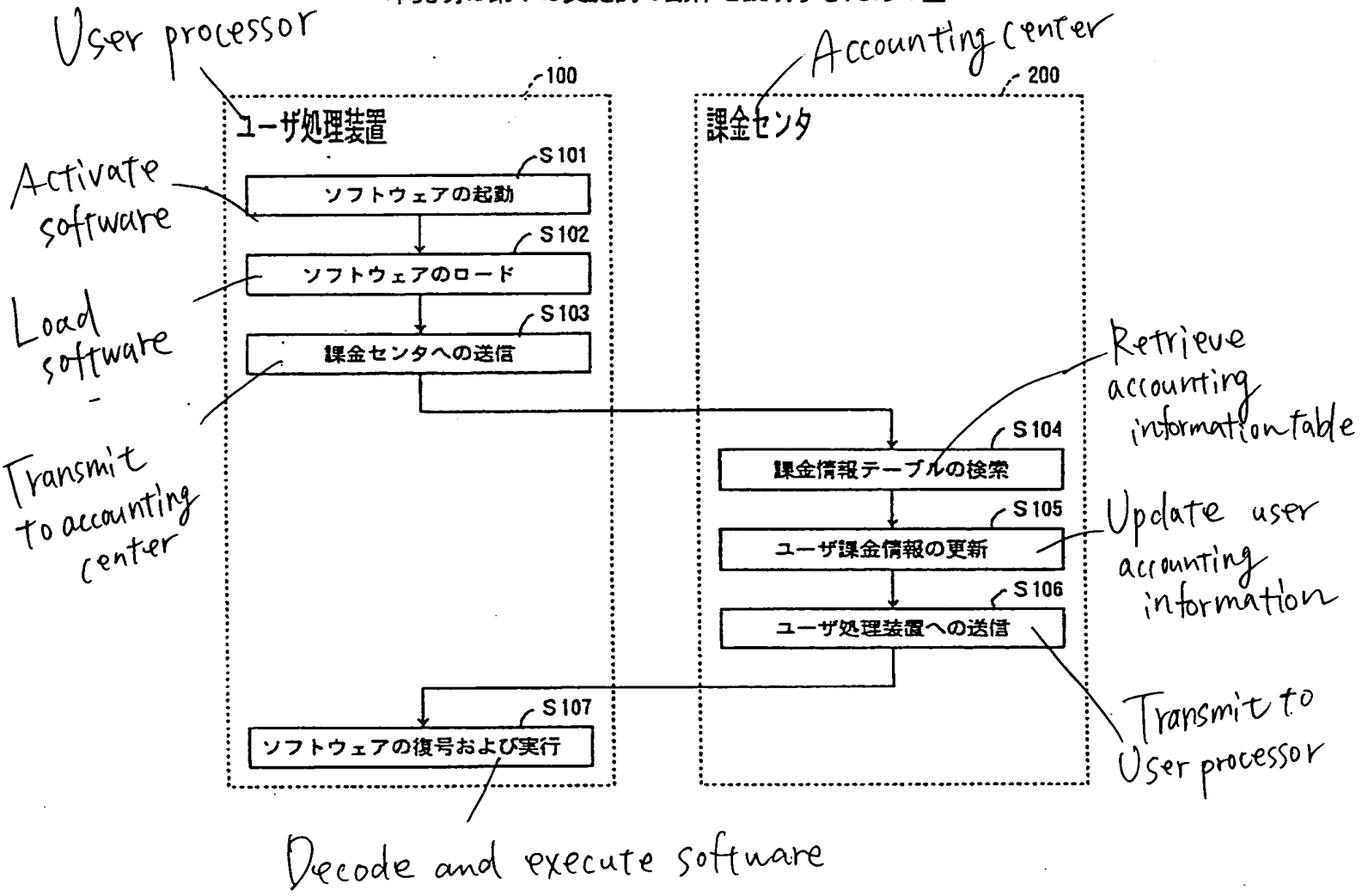
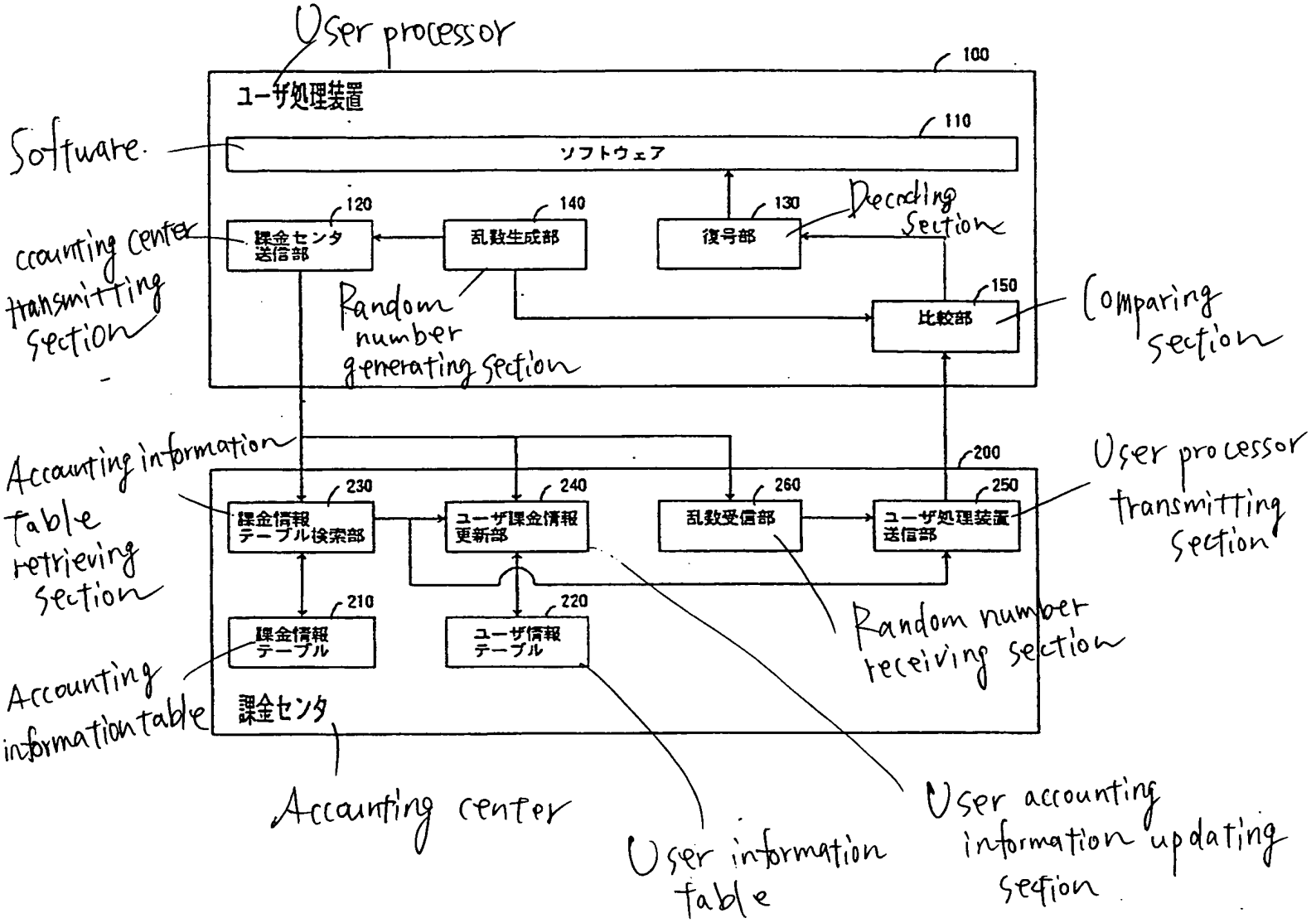


FIG. 5
Diagram illustrating structure of system according to second embodiment of the present invention

【図５】

本発明の第２の実施例のシステム構成図



【図６】

本発明の第２の実施例の動作を説明するための図

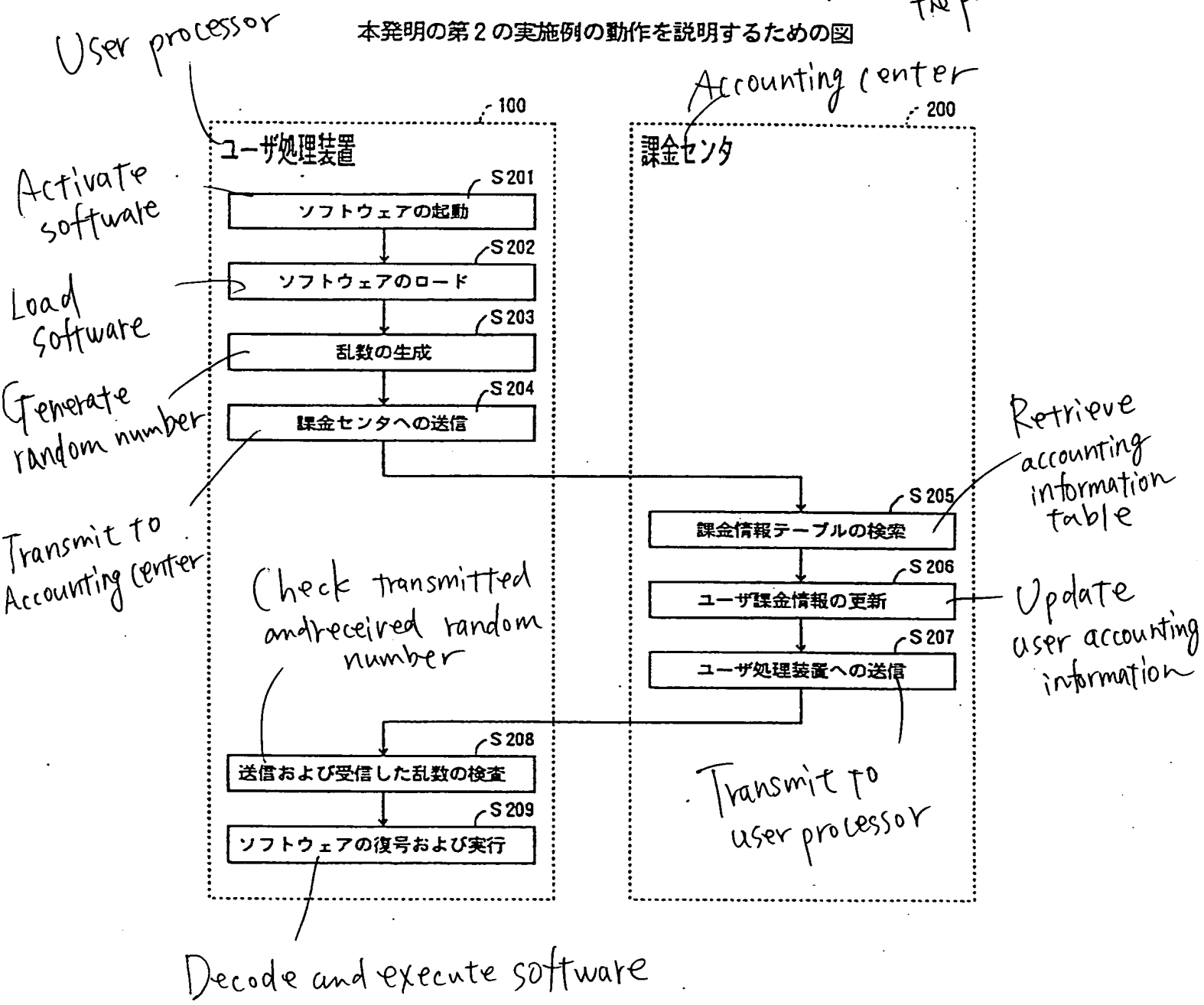


FIG 6 Diagram illustrating operation according to second embodiment of the present invention

FIG. 7

Diagram illustrating operation according to third embodiment of the present invention

【図７】

本発明の第３の実施例の動作を説明するための図

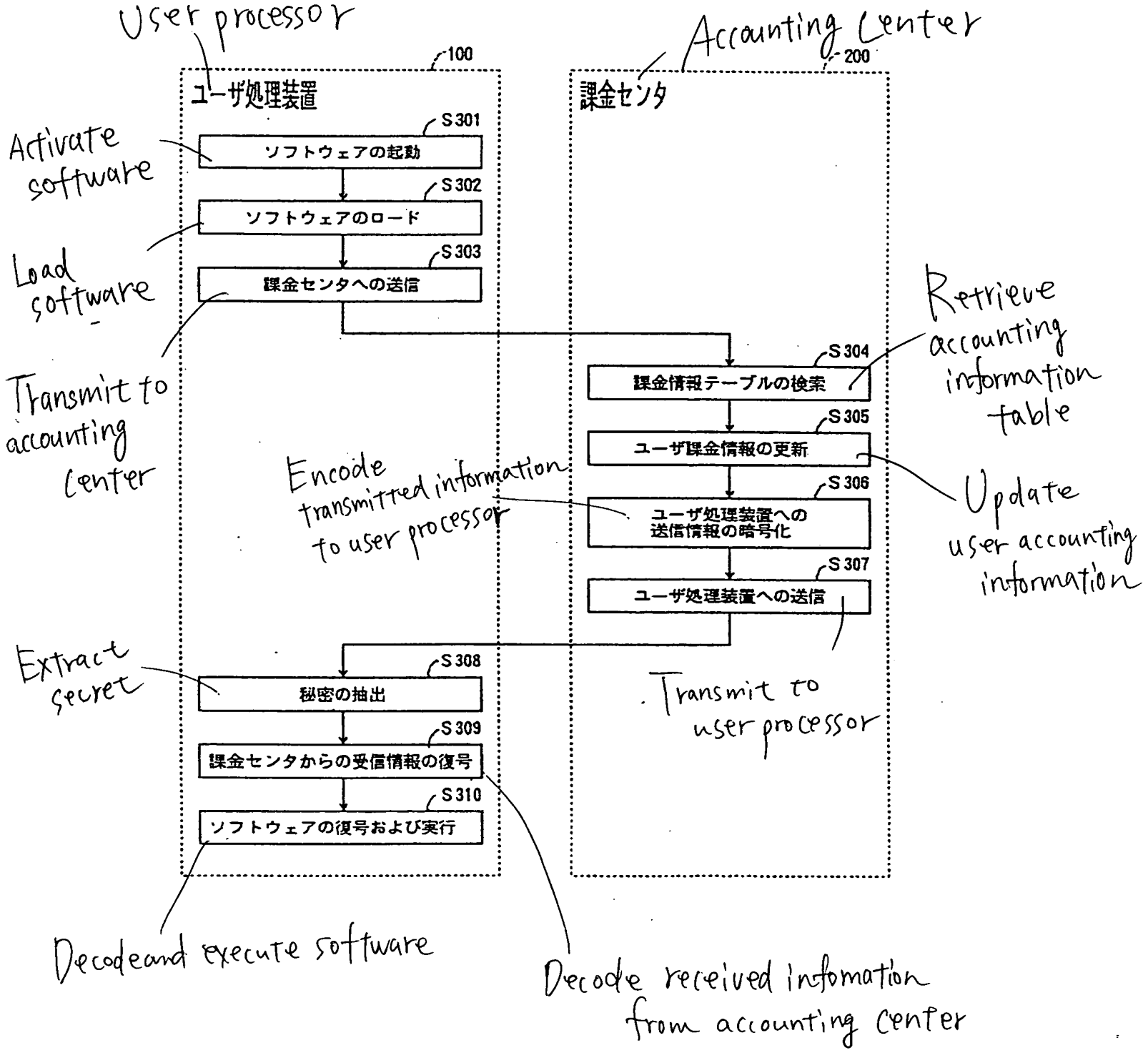


FIG. 8
Diagram illustrating structure of system according to fourth embodiment of the present invention

【図８】

本発明の第４の実施例のシステム構成図

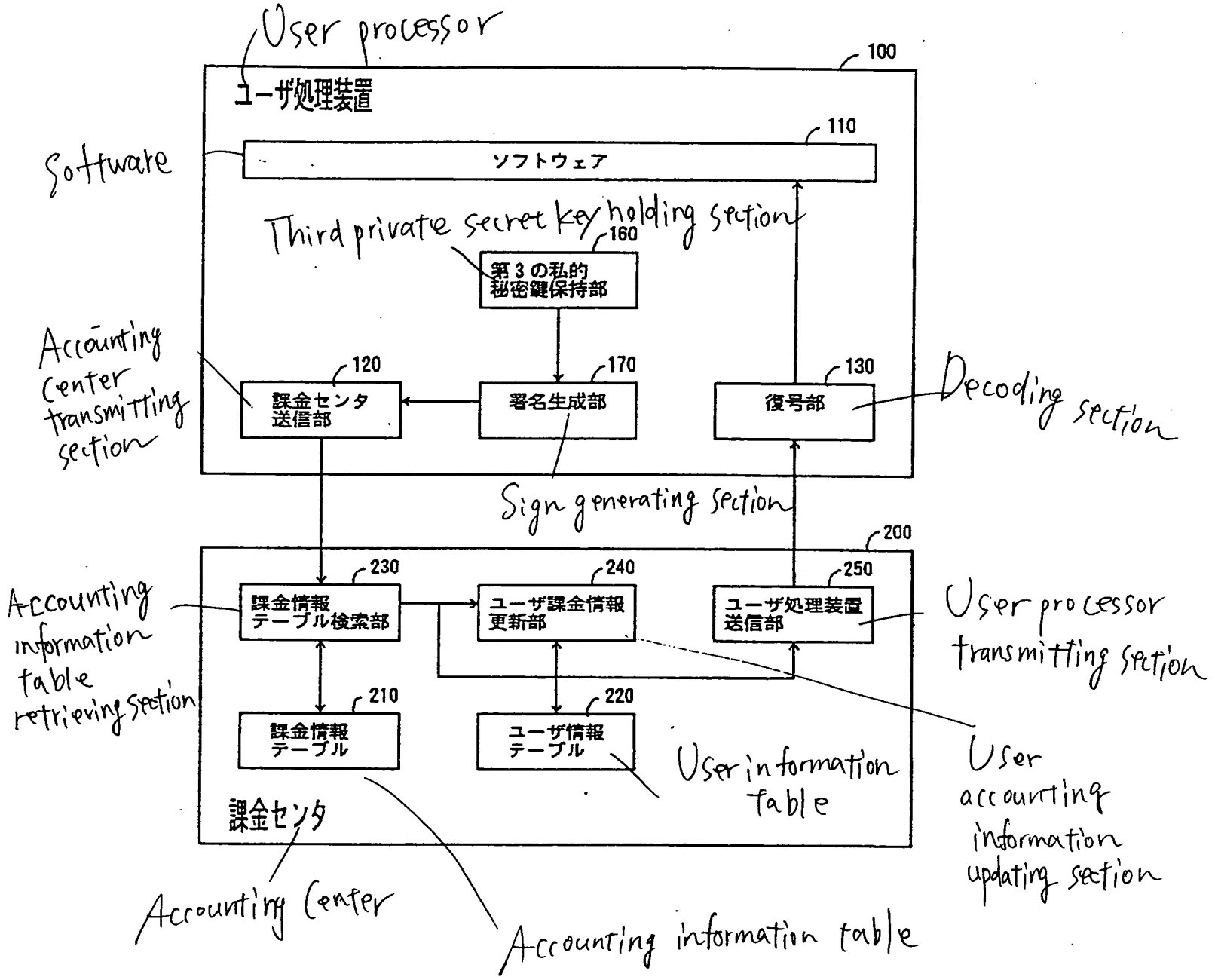


FIG.
Diagram illustrating structure of user accounting information updating section according to fourth embodiment of the present invention

【図9】

本発明の第4の実施例のユーザ課金情報更新部の構成図

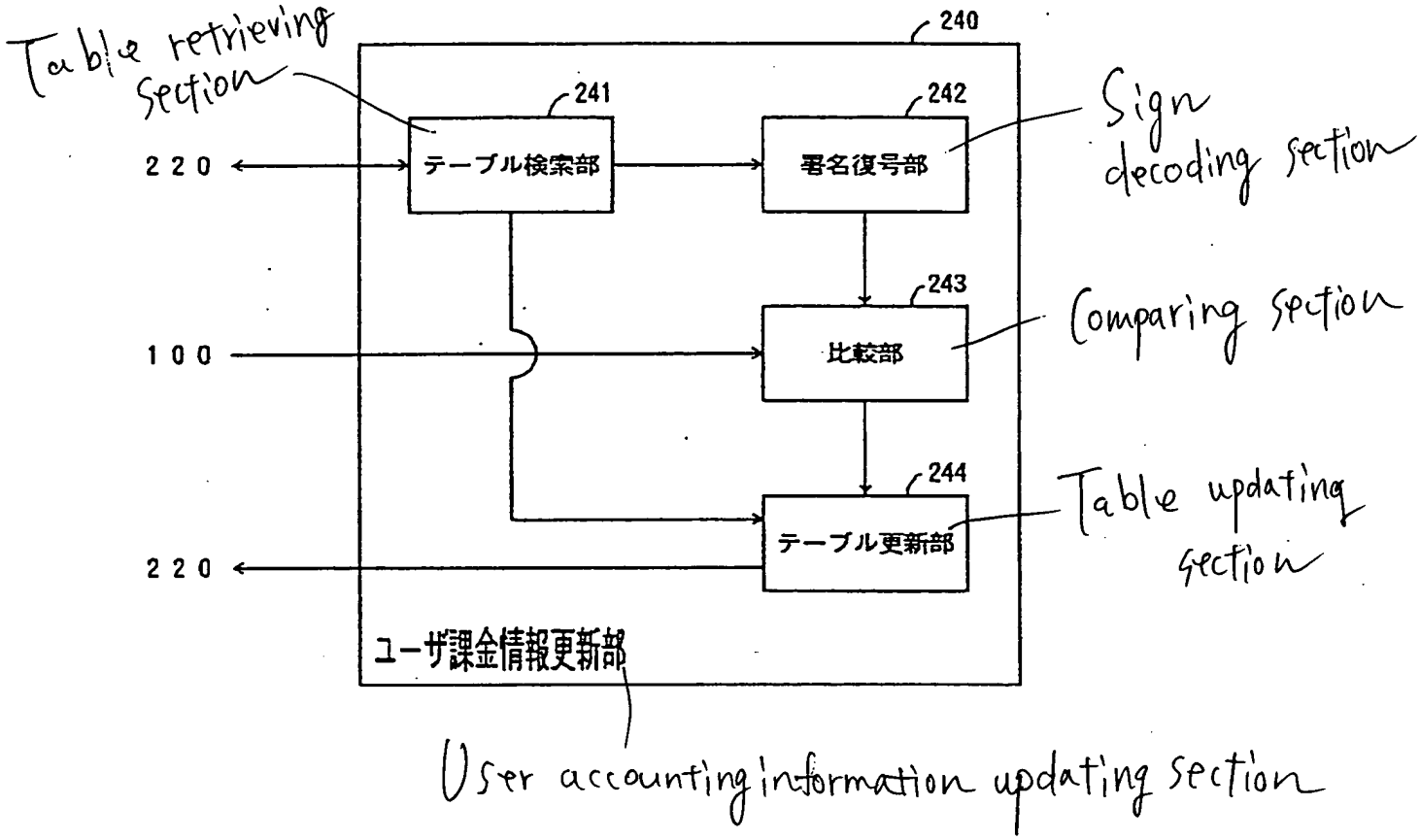


FIG. 10
Diagram illustrating operation according to fourth embodiment of the present invention

【図１０】

本発明の第４の実施例の動作を説明するための図

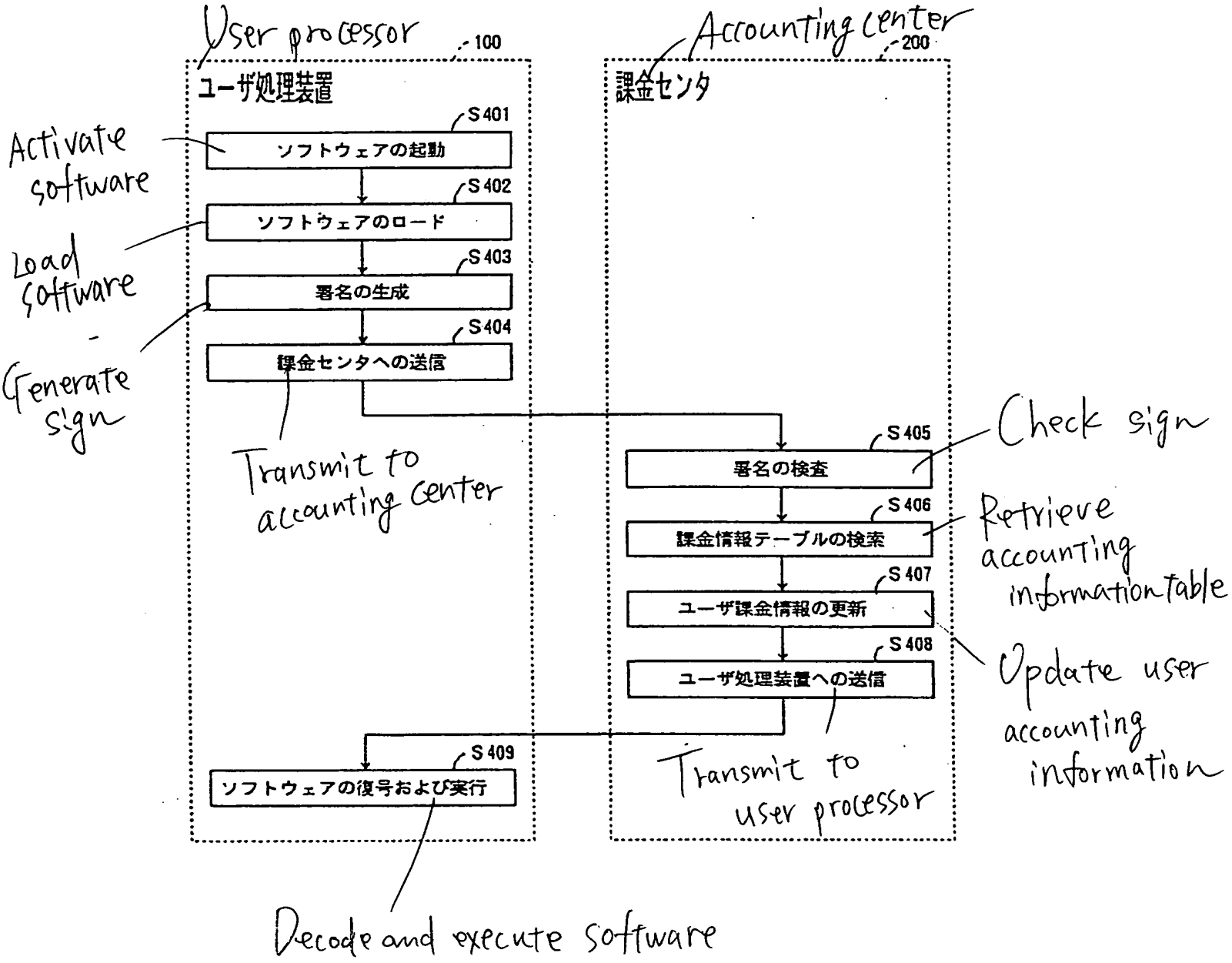


FIG. 11
Diagram illustrating operation according to fifth embodiment of the present invention

【図１１】

本発明の第５の実施例の動作を説明するための図

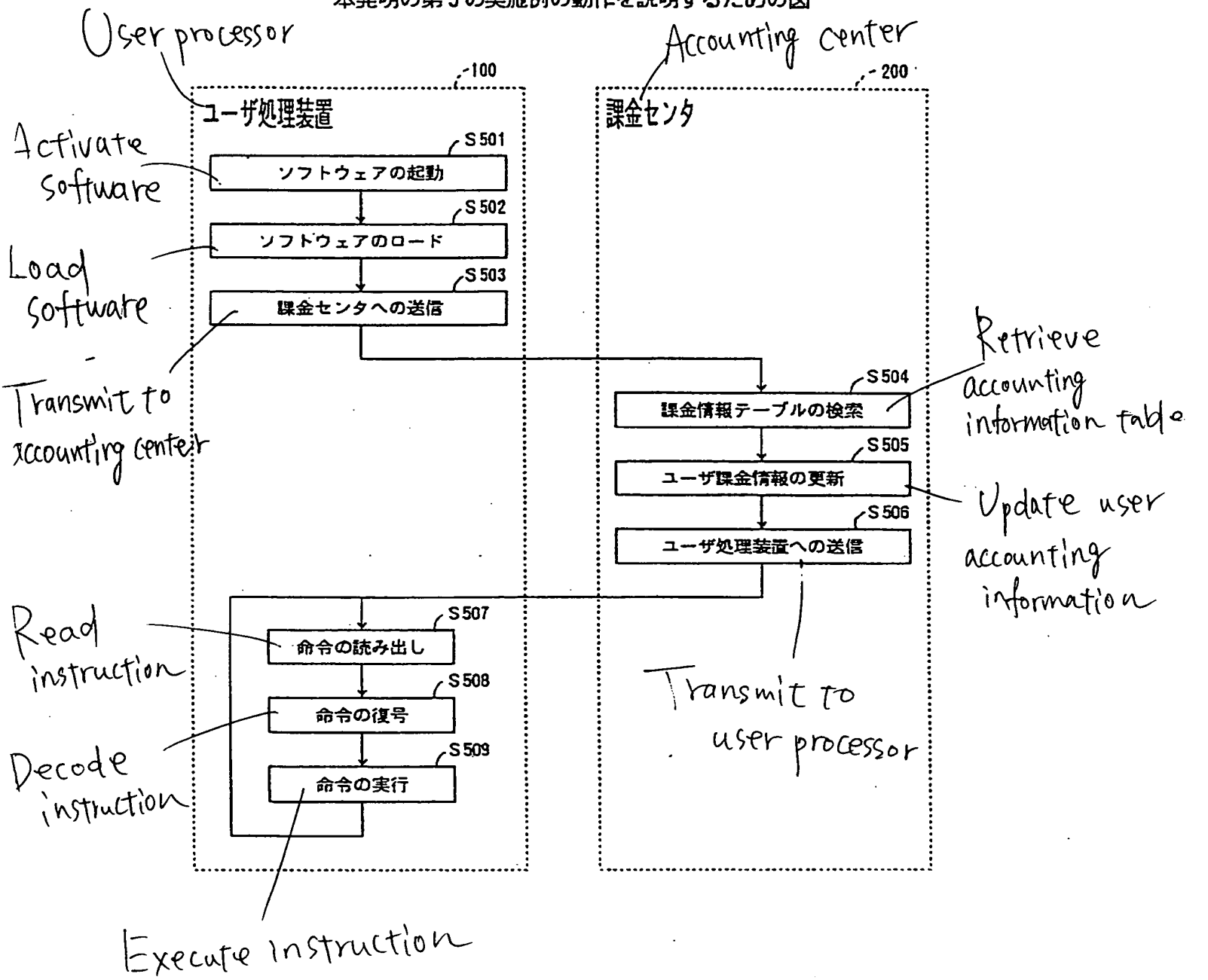


FIG. 12

Diagram illustrating structure of user processor according to sixth embodiment of the present invention

【図１２】

本発明の第６の実施例のユーザ処理装置の構成図

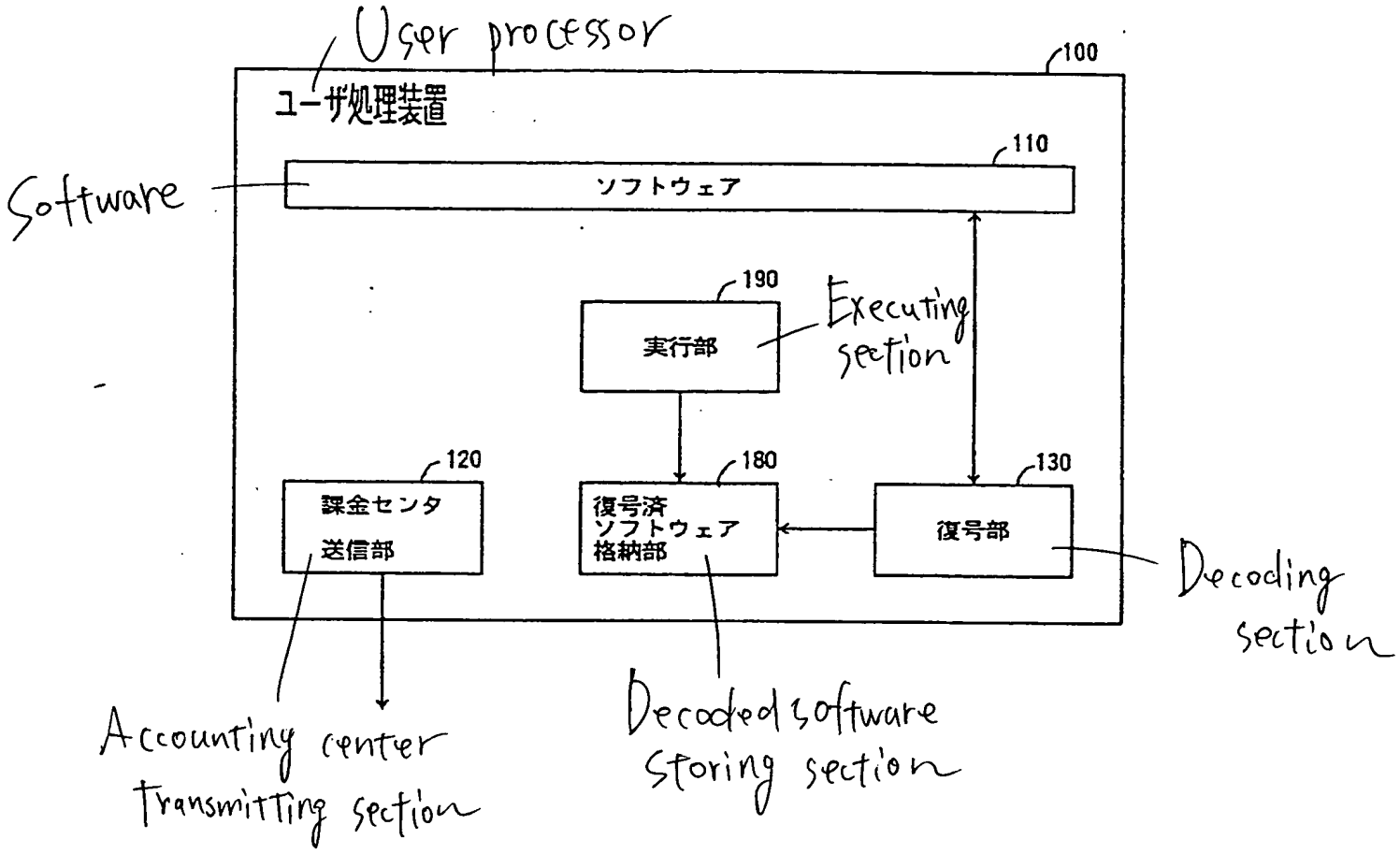


FIG. 13
Diagram illustrating operation according to sixth embodiment of the present invention

【図１３】

本発明の第６の実施例の動作を説明するための図

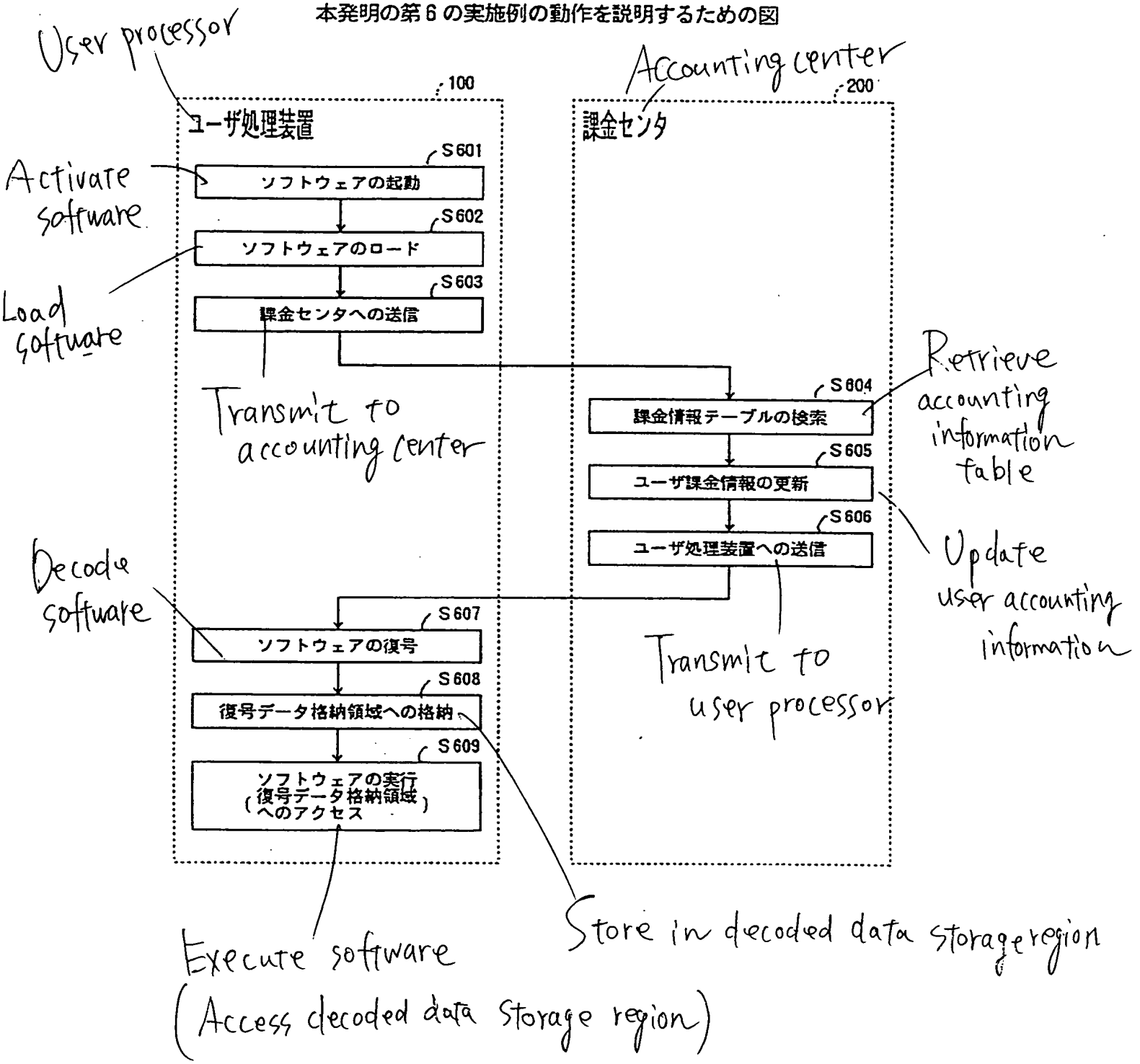
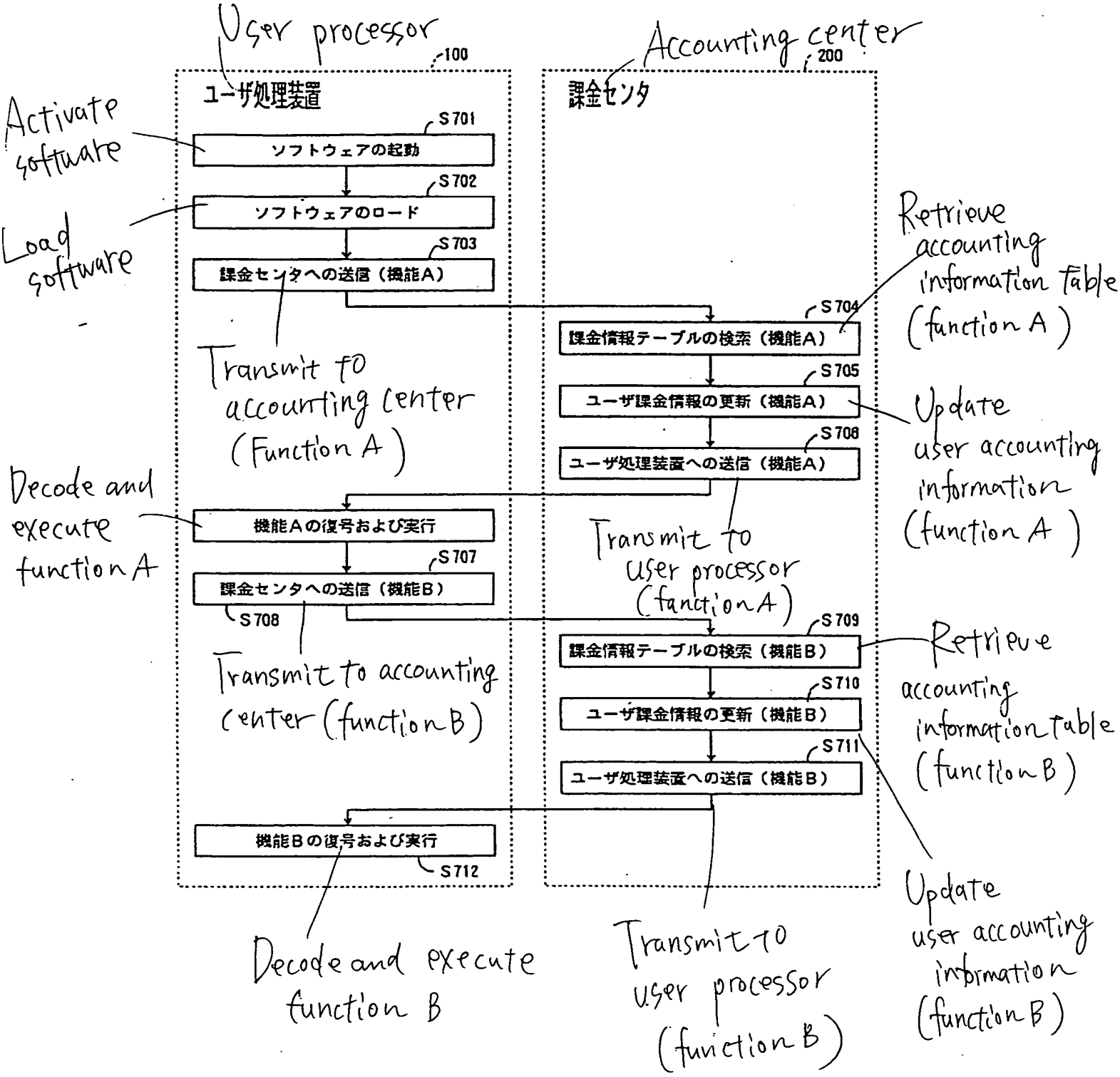


FIG. 14.
Diagram illustrating operation according to Seventh embodiment of the present invention

【図１４】

本発明の第７の実施例の動作を説明するための図



(19)日本国特許庁(JP)　(12)公開特許公報（A）　(11)特許出願公開番号

特開平１０－２０９５６

(43)公開日　平成10年(1998)1月23日

(51)Int. Cl.[6]		識別記号	庁内整理番号	FI			技術表示箇所
Ｇ０６Ｆ	1/00	３７０		Ｇ０６Ｆ	1/00	３７０　Ｆ	
	9/06	５５０			9/06	５５０　Ａ	
						５５０　Ｚ	
	13/00	３５１			13/00	３５１　Ｅ	
Ｇ０９Ｃ	1/00	６３０	7259－５Ｊ	Ｇ０９Ｃ	1/00	６３０　Ｂ	

審査請求　未請求　請求項の数２３　ＯＬ　（全２６頁）最終頁に続く

(21)出願番号　特願平8-170106

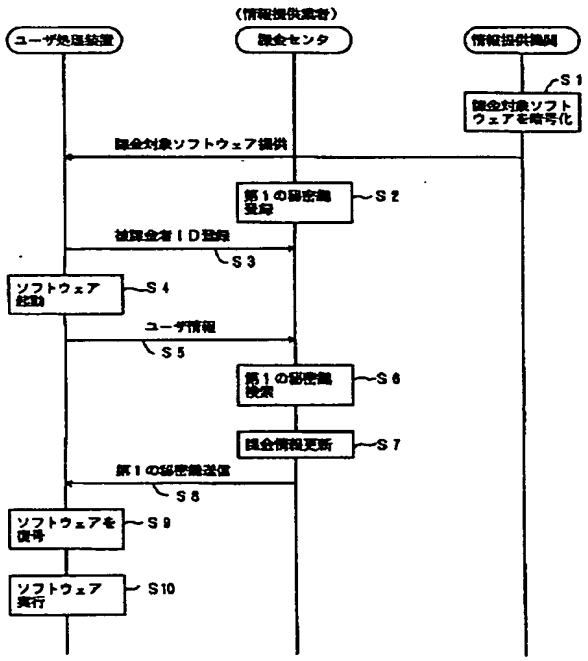
(22)出願日　平成8年(1996)6月28日

(71)出願人　000004226
日本電信電話株式会社
東京都新宿区西新宿三丁目19番2号
(72)発明者　田中　利清
東京都新宿区西新宿三丁目19番2号　日本電信電話株式会社内
(74)代理人　弁理士　伊東　忠彦

(54)【発明の名称】ソフトウェア課金方法及びシステム

(57)【要約】
【課題】　ソフトウェアの使用機能に対応し、使用回数に比例した使用量の徴収を可能にするソフトウェア課金方法及びシステムを提供することを目的とする。
【解決手段】　被課金者がソフトウェアを起動し、ユーザ情報を課金センタに送信すると、課金センタはソフトウェアの使用料及び第１の復号・秘密鍵を検索することにより取得し、被課金者ＩＤに対応する課金情報を更新し、取得した第１の復号・秘密鍵をユーザ処理装置に送信し、ユーザ処理装置は、課金センタから受信した第１の復号・秘密鍵を用いてソフトウェアの全部または、一部の暗号化されている領域を復号し、実行する。

本発明の原理を説明するための図



1

【特許請求の範囲】

【請求項１】　ユーザ処理装置に提供するソフトウェアに対する使用料を課金するためのソフトウェア課金方法において、

情報提供機関は、

被課金者に提供するソフトウェアの全部または、一部を暗号化してユーザに配付し、

課金センタは、

課金対象ソフトウェア毎に、登録情報として、ソフトウェア識別子、ソフトウェア使用料、及び暗号化されたソフトウェアを復号するための第１の復号・秘密鍵を登録しておき、

前記被課金者は、前記課金センタに被課金者ＩＤを登録しておき、

前記被課金者がソフトウェアを起動して、該ソフトウェアＩＤを含む該ソフトウェア使用通知を前記課金センタに送信すると、

前記課金センタは、前記ソフトウェア使用通知に基づいて前記ソフトウェアの使用料及び前記第１の復号・秘密鍵を検索し、

前記ソフトウェア使用料で前記被課金者ＩＤに対応する課金情報を更新し、

取得した前記第１の復号・秘密鍵をユーザ処理装置に送信し、

前記ユーザ処理装置は、前記課金センタから受信した前記第１の復号・秘密鍵を用いて前記ソフトウェアの全部または、一部の暗号化されている領域を復号し、実行することを特徴とするソフトウェア課金方法。

【請求項２】　前記ユーザ処理装置は、

乱数を生成し、前記課金センタに、前記ソフトウェア使用通知と共に送信し、

前記課金センタは、

前記ユーザ処理装置から乱数を受信し、前記第１の復号・秘密鍵と共に受信した乱数を前記ユーザ処理装置に送信し、

前記ユーザ処理装置は、

前記課金センタから前記第１の復号・秘密鍵と前記乱数を受信し、

生成した前記乱数と受信した乱数とを比較し、一致するかを判定し、一致する場合のみ前記ソフトウェアの復号を行う請求項１記載のソフトウェア課金方法。

【請求項３】　前記課金センタにおいて、

前記登録情報として、前記ソフトウェアに対応する前記第１の復号・秘密鍵を暗号化するための第２の秘密鍵を更に含み、前記第２の秘密鍵を用いて、前記ユーザ処理装置に送信する前記第１の復号・秘密鍵を暗号化した暗号化情報を前記ユーザ処理装置に送信し、

前記ユーザ処理装置では、

前記ソフトウェアに埋め込んである第２の秘密鍵を抽出し、

2

前記第２の秘密鍵を用いて、前記暗号化情報を復号して前記第１の復号・秘密鍵を取得し、

取得した前記第１の復号・秘密鍵を用いて前記ソフトウェアを復号する請求項１又は、２記載のソフトウェア課金方法。

【請求項４】　前記ユーザ処理装置は、

被課金者の第３の私的秘密鍵を用いて、前記課金センタに送信する情報の一部を暗号化することにより署名を生成して、前記課金センタに送信し、

前記課金センタは、

前記登録情報として、更に被課金者の第３の私的秘密鍵に対応した公開鍵を含み、前記署名を該公開鍵で復号した情報と、前記ユーザ処理装置から受信した他の情報と一致しているかを判定し、

一致する場合のみ前記第１の復号・秘密鍵を前記ユーザ処理処理装置に送信する請求項１、２、又は、３記載のソフトウェア課金方法。

【請求項５】　前記ユーザ処理装置では、

暗号化された前記ソフトウェアを復号して、実行する際に、命令フェッチ及びオペランド・フェッチによるメモリ・アクセスの度に、メモリから読み出した暗号化データを復号して使用する請求項１、２、３、又は４記載のソフトウェア課金方法。

【請求項６】　前記ユーザ処理装置では、

前記暗号化されたソフトウェアを復号して実行する際に、

予め、復号したデータを格納するための領域を確保し、

前記ソフトウェアの実行開始時または、実行中に、前記暗号化されたソフトウェアの全部または、一部を復号して、前記復号したデータを格納する領域に格納し、

前記ソフトウェアの実行中の復号対象領域へのアクセスは、前記復号したデータを格納する領域へのアクセスで代替する請求項１、２、３又は４記載のソフトウェア課金方法。

【請求項７】　前記ユーザ処理装置は、

前記課金センタに、前記ソフトウェアの機能ＩＤを前記ソフトウェア使用通知に付加して送信し、

前記課金センタは、

課金対象ソフトウェア毎に、ソフトウェアＩＤ、機能に対応した機能ＩＤ、機能に対応した使用料及び機能に対応した前記ソフトウェアを復号するための第４の復号・秘密鍵を登録情報として登録しておき、

前記ユーザ処理装置から送信された前記ソフトウェアＩＤ、及び前記機能ＩＤを用いて、前記登録情報を検索し、機能使用料及び、前記第４の復号・秘密鍵を取得し、

前記被課金者ＩＤ、及び前記機能使用料を用いて、前記ユーザ情報を検索して、該被課金者ＩＤに対応した課金情報を更新する請求項１、２、３、４、５又は、６記載のソフトウェア課金方法。

【請求項８】　前記情報提供機関が、ユーザに提供するソフトウェアの一部を暗号化する際に、
前記ソフトウェアのアドレス範囲内のデータを暗号化する請求項１記載のソフトウェア課金方法。
【請求項９】　前記情報提供機関が、ユーザに提供するソフトウェアの一部を暗号化する際に、
前記ソフトウェアの機能単位で暗号化する請求項１記載のソフトウェア課金方法。
【請求項１０】　前記情報提供機関が、ユーザに提供するソフトウェアの一部を暗号化する際に、
前記ソフトウェアの暗号化対象領域全ての一種類の秘密鍵で暗号化する請求項１記載のソフトウェア課金方法。
【請求項１１】　前記情報提供機関が、ユーザに提供するソフトウェアの一部を暗号化する際に、
前記ソフトウェアの暗号化対象領域を複数の副領域に分割し、
分割された各々の副領域を異なる秘密鍵で暗号化する請求項１０記載のソフトウェア課金方法。
【請求項１２】　提供されたソフトウェアを使用するユーザ処理装置と、該ユーザ処理装置が使用するソフトウェアについて課金処理を行う課金センタと、該ユーザ処理装置及び該課金センタを接続するネットワークからなるソフトウェア課金システムであって、
前記ユーザ処理装置に対して提供するソフトウェアを第１の復号・秘密鍵を用いて暗号化する第１の暗号化手段と、
暗号化されたソフトウェアを前記ユーザ処理装置に提供するソフトウェア提供手段とを有する情報提供機関を含み、
前記課金センタは、
前記ユーザ処理装置から受信したソフトウェア使用通知に基づいて、該ユーザ処理装置が使用するソフトウェアに対する課金を行う課金手段と、
前記課金処理が終了した時点で、前記第１の暗号化手段で用いられた前記第１の復号・秘密鍵を前記ユーザ処理装置に送信する復号鍵送信手段とを有し、
前記ユーザ処理装置は、
予め、前記課金センタに対して自装置ＩＤを登録するＩＤ登録手段と、
配付されたソフトウェアを使用するソフトウェア使用通知を前記課金センタに通知する使用通知手段と、
前記課金センタから受信した前記第１の復号秘密鍵を用いて、前記ソフトウェア全部、または、一部の暗号化されている領域を復号し、実行する第１の復号手段とを有することを特徴とするソフトウェア課金システム。
【請求項１３】　前記課金センタの前記課金手段は、
課金対象となるソフトウェア毎に、ソフトウェアＩＤ、ソフトウェア使用料、及び暗号化されたソフトウェアを復号するための第１の復号・秘密鍵を格納するための課金情報記憶手段と、

前記ユーザ毎に、被課金者ＩＤ及び、ユーザ課金情報を保持するユーザ情報記憶手段と、
前記ソフトウェアＩＤを用いて、前記課金情報記憶手段を検索して、ソフトウェア使用料、及び第１の復号・秘密鍵を取得する第１の検索手段と、
前記ユーザ処理装置から前記使用通知手段により送信された被課金者ＩＤに基づいて前記ユーザ情報記憶手段を検索し、該被課金者ＩＤに対応するユーザ課金情報を取得して、前記ソフトウェア使用料で更新する第１の課金情報更新手段とを含む請求項１２記載のソフトウェア課金システム。
【請求項１４】　前記ユーザ処理装置の前記通知手段は、
乱数を生成する乱数生成手段と、
前記課金センタに、前記ソフトウェア使用通知と共に、前記乱数生成手段で生成された乱数を送信する乱数送信手段とを含み、
前記第１の復号手段は、
前記課金センタから受信する乱数と前記乱数生成手段で生成された乱数とを比較し、一致するかを判定し、一致するときのみ復号を行う乱数判定手段とを含み、
前記課金センタの前記復号鍵送信手段は、
前記乱数送信手段により前記ユーザ処理装置から受信した前記乱数を前記第１の復号・秘密鍵と共に送信する乱数送信手段を含む請求項１２又は１３記載のソフトウェア課金システム。
【請求項１５】　前記課金センタの前記課金情報記憶手段は、
前記ソフトウェアに対応する前記第１の復号・秘密鍵を暗号化するための第２の秘密鍵を更に含み、
前記復号鍵送信手段は、
前記第２の秘密鍵を用いて、前記ユーザ処理装置に送信する前記第１の復号・秘密鍵を暗号化した暗号化情報を生成する第２の暗号化手段を含み、
前記ユーザ処理装置の第１の復号手段は、
前記課金センタから受信した前記暗号化情報を、前記ソフトウェアに埋め込んである第２の秘密鍵を抽出し、前記暗号化情報を該第２の秘密鍵で復号して、該第１の復号・秘密鍵を取得し、該第１の復号・秘密鍵で前記ソフトウェアを復号する第２の復号化手段を含む請求項１２、１３又は、１４記載のソフトウェア課金システム。
【請求項１６】　前記ユーザ処理装置の使用通知手段は、
被課金者の第３の私的秘密鍵を用いて、前記課金センタに送信するソフトウェア使用通知の一部を暗号化することにより署名を生成する署名生成手段と、
前記課金センタに送信する前記ソフトウェア使用通知と共に署名を前記課金センタに送信する署名送信手段を更に有し、
前記課金センタは、

前記ユーザ情報記憶手段に、被課金者の第３の私的秘密鍵に対応した公開鍵を含み、

前記ユーザ情報記憶手段上の前記被課金者の第３の私的秘密鍵に対応し、署名を復号するための公開鍵を用いて、前記ユーザ処理装置から受信した前記署名を復号し、該ユーザ処理装置から受信した前記ソフトウェア使用通知との一致を判定するユーザ情報判定手段を更に有する請求項１２、１３、１４又は１５記載のソフトウェア課金システム。

【請求項１７】　前記第１の復号化手段は、

命令フェッチ及びオペランド・フェッチによるメモリ・アクセスの度に、メモリから読み出した暗号化データを復号化して使用する手段を含む請求項１２、１３、１４、１５又は１６記載のソフトウェア課金システム。

【請求項１８】　前記第１の復号化手段は、

予め復号したデータを格納する復号データ格納手段と、

前記ソフトウェアの実行開始時、または、実行中に、暗号化されたソフトウェアの全部または、一部を復号して前記復号データ格納手段に格納し、該ソフトウェアの実行中の復号対象領域へのアクセスは、前記復号データ格納手段へのアクセスで代替する代替アクセス手段を含む請求項１２、１３、１４、１５又は１６記載のソフトウェア課金システム。

【請求項１９】　前記課金センタは、

課金対象ソフトウェア毎に、ソフトウェアＩＤ、機能に対応した機能ＩＤ、機能に対応した使用料及び機能に対応し、前記ユーザ処理装置に送信され、該課金対象ソフトウェアを復号するための第４の復号・秘密鍵を格納する第２の課金情報記憶手段と、

前記ソフトウェアＩＤ及び前記機能ＩＤを用いて、前記第２の課金情報記憶手段を検索して、機能使用料及び第４の復号・秘密鍵を取得する第２の検索手段と、

前記被課金者ＩＤ及び前記機能使用料を用いて、前記ユーザ情報記憶手段を検索して、前記被課金者ＩＤに対応したユーザ課金情報を更新する第２の課金情報更新手段を更に有し、

前記ユーザ処理装置は、

被課金者ＩＤ及びソフトウェアＩＤと共に、機能ＩＤを前記課金センタに送信するＩＤ通知手段を更に有する請求項１２、１３、１４、１５、１６、１７または、１８記載のソフトウェア課金システム。

【請求項２０】　前記情報提供機関の前記第１の暗号化手段は、

前記ソフトウェアのアドレス範囲内のデータを暗号化する手段を含む請求項１２記載のソフトウェア課金システム。

【請求項２１】　前記情報提供機関の前記第１の暗号化手段は、

前記ソフトウェアの機能単位で暗号化する手段を含む請求項１２記載のソフトウェア課金システム。

【請求項２２】　前記情報提供機関の前記第１の暗号化手段は、

前記ソフトウェアの暗号化対象領域全ての一種類の秘密鍵で暗号化する手段を含む請求項１２記載のソフトウェア課金システム。

【請求項２３】　前記情報提供機関の前記第１の暗号化手段は、

前記ユーザ処理装置に提供するソフトウェアの一部を暗号化する際に、前記ソフトウェアの暗号化対象領域を複数の副領域に分割し、分割された各々の副領域を異なる秘密鍵で暗号化する手段を含む請求項２２記載のソフトウェア課金システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ソフトウェア課金方法及びシステムに係り、特に、ＣＤ－ＲＯＭやフロッピーディスク等の媒体に格納されて配付されるソフトウェアや、ネットワークを介して配付されるソフトウェアに対して課金を行うソフトウェア課金方法及びシステムに関する。

【０００２】

【従来の技術】従来のソフトウェア課金システムには、ソフトウェアを販売し、ユーザが当該ソフトウェアを買い取られた時点で課金が終了する方法がある。また、ユーザが配付されたソフトウェアを使用する際に、課金センタに使用する旨を通知し、これにより、課金センタでは、ソフトウェアの使用に対する課金を行うシステムがある。

【０００３】また、最近では、買い取り形式の変形として暗号化されたソフトウェアをＣＤ－ＲＯＭ等の媒体または、ネットワーク経由で配付し、電話、ファクシミリ、手紙または、電子メールによる購入手続き後、復号鍵を通知する方式も採用されている。さらに、予め利用可能量が設定され、かつ、暗号化されたソフトウェアを配付して、ユーザが使用した量を日数で管理し、当該日数に基づいて課金を行う方法等がある。

【０００４】

【発明が解決しようとする課題】しかしながら、上記の買い取り方式では、流通経費を相対的に低減するためにソフトウェアの機能は肥大化し、ユーザは、殆ど使用しない機能を含め、高額の費用を負担しなければならない。また、ソフトウェアを購入して実行してみなければユーザが必要とする機能が満足されているか否かを判断できない。

【０００５】また、単に、ユーザが配付されたソフトウェアを使用する際に、課金センタに使用する旨を通知する方法では、課金は可能であってもソフトウェアの使用を制限することができないため、使用料金の未払いがあっても対処することができないという問題がある。

【０００６】暗号化されたソフトウェアを予め提供し、

使用時に復号鍵を提供するシステムであっても、使用回数に関わらず、ユーザは、同一の金額を支払う必要があり、使用回数または、使用時間当たりの価格には大きな幅がある。本発明は、上記の点に鑑みなされたもので、ソフトウェアの使用機能に対応し、使用回数に比例した使用量の徴収を可能にするソフトウェア課金方法及びシステムを提供することを目的とする。

【０００７】詳しくは、ソフトウェアの使用要求に対して、ユーザ課金情報を更新した後、使用許可を与え、使用許可されたソフトウェアがただ１回だけ使用可能であることを保障し、１回当たりの使用料を安価にすることが可能なソフトウェア課金方法及びシステムを提供することである。

【０００８】

【課題を解決するための手段】図１は、本発明の原理を説明するための図である。本発明は、ユーザ処理装置に提供するソフトウェアに対する使用料を課金するためのソフトウェア課金方法において、情報提供機関は、被課金者に提供するソフトウェアの全部または、一部を暗号化してユーザに配付し（ステップ１）、課金センタは、課金対象ソフトウェア毎に、登録情報として、ソフトウェア識別子、ソフトウェア使用料及び暗号化されたソフトウェアを復号するための第１の復号・秘密鍵を登録しておき（ステップ２）、被課金者は、課金センタに被課金者ＩＤを登録しておき（ステップ３）、被課金者がソフトウェアを起動して（ステップ４）、該ソフトウェアＩＤを含む該ソフトウェア使用通知を課金センタに送信すると（ステップ５）、課金センタは、ソフトウェア使用通知に基づいてソフトウェアの使用料及び第１の復号・秘密鍵を検索し（ステップ６）、ソフトウェア使用料で被課金者ＩＤに対応する課金情報を更新し（ステップ７）、取得した第１の復号・秘密鍵をユーザ処理装置に送信し（ステップ８）、ユーザ処理装置は、課金センタから受信した第１の復号・秘密鍵を用いてソフトウェアの全部または、一部の暗号化されている領域を復号し（ステップ９）、実行する（ステップ１０）。

【０００９】また、本発明において、ユーザ処理装置は、乱数を生成し、課金センタに、ソフトウェア使用通知と共に送信し、課金センタは、ユーザ処理装置から乱数を受信し、第１の復号・秘密鍵と共に受信した乱数をユーザ処理装置に送信し、ユーザ処理装置は、課金センタから第１の復号・秘密鍵と乱数を受信し、生成した乱数と受信した乱数とを比較し、一致するかを判定し、一致する場合のみソフトウェアの復号を行う。

【００１０】また、本発明は、課金センタにおいて、登録情報として、ソフトウェアに対応する第１の復号・秘密鍵を暗号化するための第２の秘密鍵を更に含み、第２の秘密鍵を用いて、ユーザ処理装置に送信する第１の復号・秘密鍵を暗号化した暗号化情報をユーザ処理装置に送信し、ユーザ処理装置では、ソフトウェアに埋め込んである第２の秘密鍵を抽出し、第２の秘密鍵を用いて、暗号化情報を復号して第１の復号・秘密鍵を取得し、取得した第１の復号・秘密鍵を用いてソフトウェアを復号する。

【００１１】また、本発明において、ユーザ処理装置は、被課金者の第３の私的秘密鍵を用いて、課金センタに送信する情報の一部を暗号化することにより署名を生成して、課金センタに送信し、課金センタは、登録情報として、更に被課金者の第３の私的秘密鍵に対応した公開鍵を含み、署名を該公開鍵で復号した情報と、ユーザ処理装置から受信した他の情報と一致しているかを判定し、一致する場合のみ第１の復号・秘密鍵をユーザ処理処理装置に送信する。

【００１２】また、本発明において、ユーザ処理装置では、暗号化されたソフトウェアを復号して、実行する際に、命令フェッチ及びオペランド・フェッチによるメモリ・アクセスの度に、メモリから読み出した暗号化データを復号して使用する。

【００１３】また、本発明において、ユーザ処理装置では、暗号化されたソフトウェアを復号して実行する際に、予め、復号したデータを格納するための領域を確保し、ソフトウェアの実行開始時または、実行中に、暗号化されたソフトウェアの全部または、一部を復号して、復号したデータを格納する領域に格納し、ソフトウェアの実行中の復号対象領域へのアクセスは、復号したデータを格納する領域へのアクセスで代替する。

【００１４】また、本発明において、ユーザ処理装置は、課金センタに、ソフトウェアの機能ＩＤをソフトウェア使用通知に付加して送信し、課金センタは、課金対象ソフトウェア毎に、ソフトウェアＩＤ、機能に対応した機能ＩＤ、機能に対応した使用料及び機能に対応したソフトウェアを復号するための第４の復号・秘密鍵を登録情報として登録しておき、ユーザ処理装置から送信されたソフトウェアＩＤ、及び機能ＩＤを用いて、登録情報を検索し、機能使用料及び、第４の復号・秘密鍵を取得し、被課金者ＩＤ、及び機能使用料を用いて、ユーザ情報を検索して、該被課金者ＩＤに対応した課金情報を更新する。

【００１５】また、本発明は、情報提供機関が、ユーザに提供するソフトウェアの一部を暗号化する際に、ソフトウェアのアドレス範囲内のデータを暗号化する。また、本発明は、情報提供機関が、ユーザに提供するソフトウェアの一部を暗号化する際に、ソフトウェアの機能単位で暗号化する。

【００１６】また、本発明は、情報提供機関が、ユーザに提供するソフトウェアの一部を暗号化する際に、ソフトウェアの暗号化対象領域全ての一種類の秘密鍵で暗号化する。また、本発明は、情報提供機関が、ユーザに提供するソフトウェアの一部を暗号化する際に、ソフトウェアの暗号化対象領域を複数の副領域に分割し、分割さ

れた各々の副領域を異なる秘密鍵で暗号化する。

【００１７】図２は、本発明の原理構成図である。本発明は、提供されたソフトウェアを使用するユーザ処理装置１００と、該ユーザ処理装置１００が使用するソフトウェアについて課金処理を行う課金センタ２００と、該ユーザ処理装置１００及び該課金センタ２００を接続するネットワークからなるソフトウェア課金システムであって、ユーザ処理装置１００に対して提供するソフトウェアを第１の復号・秘密鍵を用いて暗号化する第１の暗号化手段と、暗号化されたソフトウェアをユーザ処理装置１００に提供するソフトウェア提供手段とを有する情報提供機関を含み、課金センタ２００は、ユーザ処理装置１００から受信したソフトウェア使用通知に基づいて、該ユーザ処理装置１００が使用するソフトウェアに対する課金を行う課金手段２４０と、課金処理が終了した時点で、第１の暗号化手段で用いられた第１の復号・秘密鍵をユーザ処理装置１００に送信する復号鍵送信手段２５０とを有し、ユーザ処理装置１００は、予め、課金センタ２００に対して自装置ＩＤを登録するＩＤ登録手段１０１と、配付されたソフトウェアを使用するソフトウェア使用通知を課金センタ２００に通知する使用通知手段１２０と、課金センタ２００から受信した第１の復号秘密鍵を用いてソフトウェアの全部または、一部暗号化された領域を復号し、実行する第１の復号手段１３０とを有する。

【００１８】また、本発明において、課金センタ２００の課金手段２４０は、課金対象となるソフトウェア毎に、ソフトウェアＩＤ、ソフトウェア使用料、及び暗号化されたソフトウェアを復号するための第１の復号・秘密鍵を格納するための課金情報記憶手段と、ユーザ毎に、被課金者ＩＤ及び、ユーザ課金情報を保持するユーザ情報記憶手段と、ソフトウェアＩＤを用いて、課金情報記憶手段を検索して、ソフトウェア使用料、及び第１の復号・秘密鍵を取得する第１の検索手段と、ユーザ処理装置１００から使用通知手段１２０により送信された被課金者ＩＤに基づいてユーザ情報記憶手段を検索し、該被課金者ＩＤに対応するユーザ課金情報を取得して、ソフトウェア使用料で更新する第１の課金情報更新手段とを含む。

【００１９】また、本発明のユーザ処理装置１００の通知手段は、乱数を生成する乱数生成手段と、課金センタ２００に、ソフトウェア使用通知と共に、乱数生成手段で生成された乱数を送信する乱数送信手段とを含み、第１の復号手段１３０は、課金センタ２００から受信する乱数と乱数生成手段で生成された乱数とを比較し、一致するかを判定し、一致するときのみ復号を行う乱数判定手段とを含み、課金センタ２００の復号鍵送信手段２５０は、乱数送信手段によりユーザ処理装置１００から受信した乱数を第１の復号・秘密鍵と共に送信する乱数送信手段を含む。

【００２０】また、本発明の課金センタ２００の課金情報記憶手段は、ソフトウェアに対応する第１の復号・秘密鍵を暗号化するための第２の秘密鍵を更に含み、復号鍵送信手段２５０は、第２の秘密鍵を用いて、ユーザ処理装置１００に送信する第１の復号・秘密鍵を暗号化した暗号化情報を生成する第２の暗号化手段を含み、ユーザ処理装置１００の第１の復号手段１３０は、課金センタ２００から受信した暗号化情報を、ソフトウェアに埋め込んである第２の秘密鍵を抽出し、暗号化情報を復号して第１の復号・秘密鍵を取得し、該第１の復号・秘密鍵でソフトウェアを復号する第２の復号化手段を含む。

【００２１】また、本発明のユーザ処理装置１００の使用通知手段１２０は、被課金者の第３の私的秘密鍵を用いて、課金センタ２００に送信するソフトウェア使用通知の一部を暗号化することにより署名を生成する署名生成手段と、課金センタ２００に送信するソフトウェア使用通知と共に署名を課金センタ２００に送信する署名送信手段を更に有し、課金センタ２００は、ユーザ情報記憶手段に、被課金者の第３の私的秘密鍵に対応した公開鍵を含み、ユーザ情報記憶手段上の被課金者の第３の私的秘密鍵に対応し、署名を復号するための公開鍵を用いて、ユーザ処理装置１００から受信した署名を復号し、該ユーザ処理装置１００から受信したソフトウェア使用通知との一致を判定するユーザ情報判定手段を更に有する。

【００２２】また、本発明の第１の復号化手段は、命令フェッチ及びオペランド・フェッチによるメモリ・アクセスの度に、メモリから読み出した暗号化データを復号化して使用する手段を含む。また、本発明の第１の復号化手段は、予め復号したデータを格納する復号データ格納手段と、ソフトウェアの実行開始時、または、実行中に、暗号化されたソフトウェアの全部または、一部を復号して復号データ格納手段に格納し、該ソフトウェアの実行中の復号対象領域へのアクセスは、復号データ格納手段へのアクセスで代替する代替アクセス手段を含む。

【００２３】また、本発明の課金センタ２００は、課金対象ソフトウェア毎に、ソフトウェアＩＤ、機能に対応した機能ＩＤ、機能に対応した使用料及び機能に対応し、ユーザ処理装置１００に送信され、該課金対象ソフトウェアを復号するための第４の復号・秘密鍵を格納する第２の課金情報記憶手段と、ソフトウェアＩＤ及び機能ＩＤを用いて、第２の課金情報記憶手段を検索して、機能使用料及び第４の復号・秘密鍵を取得する第２の検索手段と、被課金者ＩＤ及び機能使用料を用いて、ユーザ情報記憶手段を検索して、被課金者ＩＤに対応したユーザ課金情報を更新する第２の課金情報更新手段を更に有し、ユーザ処理装置１００は、被課金者ＩＤ及びソフトウェアＩＤと共に、機能ＩＤを課金センタ２００に送信するＩＤ通知手段を更に有する。

【００２４】また、本発明の情報提供機関の第１の暗号

化手段は、ソフトウェアのアドレス範囲内のデータを暗号化する手段を含む。また、本発明の情報提供機関の第１の暗号化手段は、ソフトウェアの機能単位で暗号化する手段を含む。

【００２５】また、本発明の情報提供機関の第１の暗号化手段は、ソフトウェアの暗号化対象領域全ての一種類の秘密鍵で暗号化する手段を含む。また、本発明の情報提供機関の第１の暗号化手段は、ユーザ処理装置１００に提供するソフトウェアの一部を暗号化する際に、ソフトウェアの暗号化対象領域を複数の副領域に分割し、分割された各々の副領域を異なる秘密鍵で暗号化する手段を含む。

【００２６】上記の各発明では、予め、ユーザに提供するソフトウェアの全部または、一部が、当該ソフトウェアの開発時または、提供の前に暗号化されているものとする。このソフトウェアの一部を暗号化する場合には、あるアドレスの範囲内のデータを暗号化してもよいし、命令部、または、データ部を暗号化してもよいし、あるいは、機能の単位で暗号化してもよい。また、暗号化対象領域の全てを一種類の秘密鍵で暗号化してもよいし、暗号化対象領域を複数の副領域に分け、それぞれの副領域を異なる秘密鍵で暗号化してもよい。このように、種々の方法により暗号化が可能である。

【００２７】また、本発明では、ソフトウェアの提供前に、課金センタの課金情報記憶手段に、ソフトウェアＩＤと、ソフトウェア使用料、及び上記の暗号化されたソフトウェアを復号するための秘密鍵を登録しておく。さらに、ユーザは、ソフトウェアの使用に先立ち、課金センタのユーザ情報テーブルに被課金者ＩＤを登録しておく。

【００２８】ユーザがユーザ処理装置上でソフトウェアを起動し、ソフトウェアの実行前または、実行中に、当該ユーザ処理装置から、ソフトウェアＩＤ及び被課金者ＩＤを課金センタに送信すると、課金センタでは課金情報記憶手段を、ユーザ処理装置から受信したソフトウェアＩＤを用いて検索し、ソフトウェアの使用料及び復号するための秘密鍵を取得する。次に、課金センタのユーザ課金情報を、ユーザ処理装置から受信した被課金者ＩＤを用いてユーザ情報記憶手段を検索し、課金情報テーブルから取得したソフトウェア使用料を用いて被課金者のユーザ課金情報を更新することにより、被課金者毎の課金処理を行う。さらに、課金センタは、ユーザ処理装置に課金情報記憶手段から取得した復号するための秘密鍵を送信する。これにより、ユーザ処理装置は、課金センタから受信した秘密鍵を用いて、ソフトウェアの全部または、一部の暗号化されている領域を復号して実行する。

【００２９】これにより、情報提供機関から暗号化されたソフトウェアを提供し、ユーザが当該ソフトウェアを実行する（起動する）際に、課金センタにおいて課金処理を行い、当該ソフトウェアを使用するための秘密鍵を送信することにより、ユーザに当該ソフトウェアの使用を許可する。

【００３０】さらに、ソフトウェアの一部を暗号化して送信することにより、ユーザが全てのソフトウェアを利用しない場合に、ユーザは、使用しないソフトウェアに対する支払いを行う必要がない。また、本発明は、ユーザ処理装置において生成した乱数を課金センタに送信し、課金センタから返却された乱数とを照合して、一致する場合のみソフトウェアの復号を行うことにより、第三者の不正使用を防止する。

【００３１】また、本発明は、ソフトウェアを復号するための第１の復号秘密鍵を更に暗号化した暗号化情報をユーザ処理装置に送信し、ユーザ処理装置では、当該暗号化情報を復号して取得した第１の復号鍵を用いて、ソフトウェアを復号して実行することにより、ユーザは、課金センタから受信した暗号化情報を復号できない限りソフトウェアを復号することができない。

【００３２】また、本発明は、ユーザ処理装置において署名を生成して課金センタに送信し、課金センタにおいて、署名を復号した情報と受信した他の情報が一致しているかを判定し、不一致の場合にはユーザ処理装置に第１の復号秘密鍵を送信しないため、悪意の第三者が別の署名を送信した場合には、ソフトウェアを復号し、実行することができない。

【００３３】また、本発明は、復号されたデータを格納する領域を設定しておくことにより、復号されたソフトウェアを順次当該領域に格納しておくことにより、実行時におけるソフトウェアのアクセスを当該領域に対して行うことにより、既に復号されているソフトウェアが格納されているため効率のよいアクセスが可能となる。

【００３４】また、本発明は、ユーザ処理装置から課金センタにソフトウェアＩＤや被課金者ＩＤと共に、ソフトウェアの機能ＩＤを併せて送信することにより、起動するソフトウェア内の機能群単位に課金することが可能となる。

【００３５】

【発明の実施の形態】図３は、本発明のシステム構成図である。以下に説明するシステムは、ユーザ処理装置１００と課金センタ２００及び当該ユーザ処理装置１００と課金センタ２００を接続する通信網（図示せず）から構成される。

【００３６】なお、課金センタ２００は、当該ソフトウェアを提供する情報提供業者であり、課金システムを実行することから便宜的に課金センタと記すものとするが、情報提供業者と課金センタは別個に独立して設定されていもよい。ユーザ処理装置１００は、課金センタ送信部１２０と復号部１３０とを有し、復号部１３０は、課金対象となるソフトウェア１１０を復号鍵（以下、第１の復号・秘密該）を用いて復号する。ソフトウェア１

１０は、その全部または、一部が１つまたは、複数の秘密鍵を用いて暗号化されているものであり、予め課金センタ２００（情報提供業者）から提供されているものとする。

【００３７】課金センタ送信部１２０は、自装置の被課金者ＩＤ等のユーザ情報及び起動するソフトウェアＩＤを送信する。課金センタ２００は、課金情報テーブル２１０、ユーザ情報テーブル２２０、課金情報テーブル検索部２３０、ユーザ課金情報更新部２４０、ユーザ処理装置送信部２５０とを有する。

【００３８】課金情報テーブル２１０は、ソフトウェアＩＤ，ソフトウェア使用料、暗号化されたソフトウェアを復号するための第１の復号秘密鍵から構成される。なお、以下の説明では、情報提供業者から、予め、ユーザ処理装置１００に配付するためのソフトウェアの全部または、一部を暗号化してユーザ処理装置１００に送信し、暗号化時に使用した秘密鍵を第１の復号秘密鍵として、課金センタ２００の課金情報テーブル２１０に登録しておくものとする。

【００３９】ユーザ情報テーブル２２０は、ユーザ処理装置１００から転送された被課金者ＩＤと、ユーザ課金情報とから構成される。課金情報テーブル検索部２３０は、ユーザ処理装置１００から受信したソフトウェアＩＤを用いて課金情報テーブル２１０を検索し、当該ソフトウェアの使用料を取得し、ユーザ課金情報更新部２４０に転送し、さらに、検索により、第１の復号秘密鍵を取得して、ユーザ処理装置送信部２５０に転送する。

【００４０】ユーザ課金情報更新部２４０は、ユーザ処理装置１００から受信した被課金者ＩＤを用いてユーザ情報テーブル２２０を検索し、当該被課金者のユーザ課金情報を取得し、ソフトウェアの使用料で更新する。ユーザ処理装置送信部２５０は、課金情報テーブル検索部２３０から取得した第１の復号秘密鍵をユーザ処理装置１００に転送する。

【００４１】

【実施例】以下、図面と共に、本発明の実施例を詳細に説明する。

［第１の実施例］本実施例におけるシステム構成は、前述の図３に示すシステム構成によるものである。

【００４２】図４は、本発明の第１の実施例の動作を説明するための図である。

ステップ１０１）　ユーザ処理装置１００は、予め、情報提供業者から提供されたソフトウェア１１０を起動させる。

ステップ１０２）　当該ソフトウェア１１０をメモリ上にロードする。

【００４３】ステップ１０３）　ユーザ処理装置１００において、予め暗号化されたソフトウェア１１０を起動すると、ユーザ処理装置１００の課金センタ送信部１２０は、ソフトウェアＩＤと被課金者ＩＤとを課金センタ２００に送信する。

ステップ１０４）　課金センタ２００は、ユーザ処理装置１００からソフトウェアＩＤと被課金者ＩＤとを受信し、課金情報テーブル検索部２３０は、ソフトウェアＩＤを用いて課金情報テーブル２１０を検索し、当該ソフトウェアＩＤに対応するソフトウェアの使用料と、第１の復号秘密鍵とを取得する。

【００４４】ステップ１０５）　ユーザ課金情報更新部２４０は、受信した被課金者ＩＤを用いて、ユーザ情報テーブル２２０を検索し、当該被課金者のユーザ課金情報を取得し、課金情報テーブル検索部２３０で検索されたソフトウェアの使用料を用いて、ユーザ課金情報を更新する（ソフトウェアの使用料をユーザ課金情報に加算する）。

【００４５】ステップ１０６）　ユーザ処理装置送信部２５０は、課金情報テーブル検索部２３０で検索された第１の復号秘密鍵をユーザ処理装置１００に送信する。

ステップ１０７）　ユーザ処理装置１００は、課金センタ２００から受信した第１の復号秘密鍵を用いて、ソフトウェアの全部または、一部の暗号化されている領域を復号して実行する。

【００４６】このように、本実施例によれば、ユーザ処理装置１００からソフトウェア使用通知としてソフトウェアＩＤと被課金者ＩＤを課金センタ２００に送出することにより、課金センタからソフトウェアを復号するための第１の復号・秘密鍵を受け取り、暗号化されているソフトウェアを復号して実行することができる。

【００４７】［第２の実施例］本実施例は、乱数を用いてソフトウェアの復号を許可することが可能か否かを判定する処理を前述の第１の実施例に付加したものである。図５は、本発明の第２の実施例のシステム構成図である。同図において、図３と同一構成部分には、同一符号を付し、その説明を省略する。

【００４８】同図に示す構成は、前述の図３のシステム構成において、ユーザ処理装置１００に乱数を生成する乱数生成部１４０と比較部１５０とを具備し、課金センタ２００に乱数受信部２６０を具備する構成である。ユーザ処理装置１００の乱数生成部１４０は、乱数を生成し、当該乱数を課金センタ送信部１２０に転送し、課金センタ送信部１２０から課金センタ２００に送信する。比較部１５０は、課金センタ２００から戻された乱数と、乱数生成部１４０で生成された乱数と課金センタ２００から返却された乱数とを比較し、一致している場合に、復号部１２０に対してソフトウェア１００の復号を許可する。

【００４９】課金センタ２００の乱数受信部２６０は、ユーザ処理装置１００から取得した乱数をユーザ処理装置送信部２５０を介してユーザ処理装置１００に戻す処理を行う。

【００５０】図６は、本発明の第２の実施例の動作を説

明するための図である。
ステップ２０１）　ユーザ処理装置１００は、予め情報提供業者から提供されたソフトウェア１１０を起動させる。
ステップ２０２）　当該ソフトウェア１１０をメモリ上にロードする。
【００５１】ステップ２０３）　乱数生成部１４０は、乱数を生成し、課金センタ送信部１２０に転送する。
ステップ２０４）　課金センタ送信部１２０は、ソフトウェアＩＤと被課金者ＩＤ及び、乱数とを課金センタ２００に送信する。
【００５２】ステップ２０５）　課金センタ２００において、乱数受信部２６０は、乱数を受信し、第１の実施例と同様に、ユーザ処理装置１００からソフトウェアＩＤと被課金者ＩＤを受信し、課金情報テーブル検索部２３０は、ソフトウェアＩＤを用いて課金情報テーブル２１０を検索し、当該ソフトウェアＩＤに対応するソフトウェアの使用料と、第１の復号秘密鍵とを取得する。
【００５３】ステップ２０６）　ユーザ課金情報更新部２４０は、受信した被課金者ＩＤ用いて、ユーザ情報テーブル２２０を検索し、当該被課金者のユーザ課金情報を取得し、課金情報テーブル検索部２３０で検索されたソフトウェアの使用料を用いて、ユーザ課金情報を更新する（ソフトウェアの使用料をユーザ課金情報に加算する）。
【００５４】ステップ２０７）　ユーザ処理装置送信部２５０は、課金情報テーブル検索部２３０で検索された第１の復号秘密鍵と乱数受信部２６０で受信した乱数をユーザ処理装置１００に送信する。
ステップ２０８）　ユーザ処理装置１００は、課金センタ２００から受信した乱数とステップ２０３で生成された乱数とを比較し、一致する場合には、復号部１３０において、課金センタ２００から受信した第１の復号秘密鍵を用いて、ソフトウェアの全部または、一部の暗号化されている領域を復号して実行する。
【００５５】本実施例では、ユーザ処理層１００から課金センタ２００に送信した乱数と、課金センタ２００から受信した乱数とが一致したときのみソフトウェアの復号を可能とする。
［第３の実施例］本実施例のシステム構成は、基本的に図３に示す構成と同様であるが、課金情報テーブル２１０において、第２の秘密鍵を保持し、課金情報テーブル検索部２３０においてソフトウェアＩＤに基づいて当該第２の秘密鍵を検索し、ユーザ課金情報更新部２４０において、第１の復号・秘密鍵を暗号化する点において異なる。
【００５６】図７は、本発明の第３の実施例の動作を説明するための図である。
ステップ３０１）　ユーザ処理装置１００は、予め、情報提供業者から提供されたソフトウェア１１０を起動させる。
ステップ３０２）　当該ソフトウェア１１０をメモリ上にロードする。
【００５７】ステップ３０３）　課金センタ送信部１２０は、ソフトウェアＩＤと被課金者ＩＤを課金センタ２００に送信する。
ステップ３０４）　課金センタ２００は、ユーザ処理装置１００からソフトウェアＩＤと被課金者ＩＤを受信し、課金情報テーブル検索部２３０は、ソフトウェアＩＤを用いて課金情報テーブル２１０を検索し、当該ソフトウェアＩＤに対応するソフトウェアの使用料、第１の復号秘密鍵及び、第２の秘密鍵とを取得する。
【００５８】ステップ３０５）　ユーザ課金情報更新部２４０は、受信した被課金者ＩＤを用いて、ユーザ情報テーブル２２０を検索し、当該被課金者のユーザ課金情報を取得し、課金情報テーブル検索部２３０で検索されたソフトウェアの使用料を用いて、ユーザ課金情報を更新する（ソフトウェアの使用料をユーザ課金情報に加算する）。
【００５９】ステップ３０６）　さらに、ユーザ課金情報更新部２４０は、第１の復号秘密鍵を課金情報テーブル２１０から取得した第２の秘密鍵を用いて暗号化し、ユーザ処理装置送信部２５０に転送する。
ステップ３０７）　ユーザ処理装置送信部２５０は、ユーザ課金情報更新部２４０で暗号化された情報をユーザ処理装置１００に送信する。
【００６０】ステップ３０８）　ユーザ処理装置１００の復号部１３０は、課金センタ２００から受信した暗号化された情報、ソフトウェア１１０に埋め込まれている第２の秘密鍵を用いて復号し、第１の復号秘密鍵を取得する。
ステップ３０９）　さらに、復号部１３０は、ステップ３０８で復号することにより取得した第１の復号秘密鍵を用いて、ソフトウェアの全部または、一部の暗号化されている領域を復号して実行する。
【００６１】このように、本実施例によれば、第１の復号・秘密鍵を暗号化してユーザ処理装置に送信することにより、より安全な第１の復号・秘密鍵を送信することができる。
［第４の実施例］図８は、本発明の第４の実施例のシステム構成図である。同図において、図３と同一構成部分には、同一符号を付し、その説明を省略する。
【００６２】図８に示すシステムにおいて、図３と異なる構成は、ユーザ処理装置１００においては、第３の私的秘密鍵保持部１６０と署名生成部１７０を含む点である。第３の私的秘密鍵保持部１６０は、署名を生成するための第３の私的秘密鍵を保持する。署名生成部１７０は、第３の私的秘密鍵を用いて署名を生成する。
【００６３】また、課金センタ２００のユーザ情報テーブル２２０は、被課金者ＩＤ、課金情報に加えて、署名

を復号するための公開鍵を保持する。図９は、本発明の第４の実施例のユーザ課金情報更新部の詳細な構成を示す。同図に示すユーザ課金情報更新部２４０は、ユーザ情報テーブルを検索し、公開鍵を取得するテーブル検索部２４１、ユーザ処理装置１００から取得した署名を公開鍵を用いて復号する署名復号部２４２、ユーザ処理装置１００から受信した他の情報と復号された情報とが一致しているかを比較する比較部２４３、ユーザ情報テーブル２２０を更新するテーブル更新部２４４から構成される。

【００６４】テーブル更新部２４４は、比較部２４３において、復号化情報と、ユーザ処理装置１００から受信した情報が一致している場合に限り、被課金者のユーザ課金情報を課金情報テーブル検索部２３０から取得したソフトウェア使用料で更新し、さらに、テーブル検索部２４１から取得した、第１の復号秘密鍵をユーザ処理装置送信部２５０に転送する。

【００６５】図１０は、本発明の第４の実施例の動作を説明するための図である。

ステップ４０１）　ユーザ処理装置１００は、予め、情報提供業者から提供されたソフトウェア１１０を起動させる。

ステップ４０２）　当該ソフトウェア１１０をメモリ上にロードする。

【００６６】ステップ４０３）　ユーザ処理装置１００の署名生成部１７０は、第３の私的秘密鍵保持部１６０から第３の私的秘密鍵を読み出して、ソフトウェアＩＤ，被課金者ＩＤとの一部を当該第３の私的秘密鍵を用いて暗号化することにより、署名を生成し、課金センタ送信部１２０に転送する。

【００６７】ステップ４０４）　課金センタ送信部１２０は、暗号化されたソフトウェアＩＤと被課金者ＩＤを課金センタ２００に送信する。

ステップ４０５）　ユーザ課金情報更新部２４０のテーブル検索部２４１は、受信した暗号化情報に対して、ユーザ情報テーブル２２０を検索して公開鍵を取得して署名復号部２４２に転送する。署名復号部２４２は、当該被課金者の公開鍵を取得し、当該暗号化情報を公開鍵で復号し、比較部２４３に転送する。比較部２４３は、ユーザ処理装置１００から受信した他の情報と比較し、一致しているかを判定する。一致している場合には、次のステップに移行する。

【００６８】ステップ４０６）　課金センタ２００の課金情報テーブル検索部２３０は、ユーザ処理装置１００から受信したソフトウェアＩＤと被課金者ＩＤを用いて、課金情報テーブル２１０を検索し、当該ソフトウェアＩＤに対応するソフトウェアの使用料、第１の復号秘密鍵とを取得する。

【００６９】ステップ４０７）　ユーザ課金情報更新部２４０のテーブル更新部２４４は、課金情報テーブル検索部２３０からユーザ課金情報を取得し、課金情報テーブル検索部２３０で検索されたソフトウェアの使用料を用いて、ユーザ課金情報を更新する（ソフトウェアの使用料をユーザ課金情報に加算する）。

【００７０】ステップ４０８）　さらに、ユーザ課金情報更新部２４０は、第１の復号秘密鍵をユーザ処理装置送信部２５０に転送し、ユーザ処理装置送信部２５０は、ユーザ課金情報更新部２４０で暗号化された情報をユーザ処理装置１００に送信する。

【００７１】ステップ４０９）　ユーザ処理装置１００の復号部１３０は、第１の復号秘密鍵を用いてソフトウェアの全部または、一部の暗号化されている領域を復号して実行する。なお、本発明は、前述の各実施例と組み合わせて実行することも可能である。これにより、署名と一致しない場合には、課金センタ２００からユーザ処理装置１００に第１の復号・秘密鍵を送信しないため、正当な署名を持たない限り、ユーザは、ソフトウェアを復号できない。

【００７２】［第５の実施例］本実施例におけるシステム構成は、図３と基本的に同様である。図１１は、本発明の第５の実施例の動作を説明するための図である。

ステップ５０１）　ユーザ処理装置１００において、予め命令部分が暗号化されたソフトウェア１１０を起動する。

【００７３】ステップ５０２）　ユーザ処理装置１００は、ソフトウェア１００をロードする。

ステップ５０３）　ユーザ処理装置１００の課金センタ送信部１２０は、ソフトウェアＩＤ，被課金者ＩＤとを課金センタ２００に送信する。

【００７４】ステップ５０４）　課金センタ２００の課金情報テーブル検索部２３０は、ユーザ処理装置１００から受信したソフトウェアＩＤを用いて課金情報テーブル２１０を検索し、当該ソフトウェアの使用料と、第１の復号秘密鍵とを取得する。

ステップ５０５）　ユーザ課金情報更新部２４０は、ユーザ処理装置１００から受信した被課金者ＩＤを用いてユーザ情報テーブル２２０を検索し、被課金者のユーザ課金情報を課金情報テーブル２１０から取得したソフトウェア使用料で更新する。

【００７５】ステップ５０６）　ユーザ処理装置送信部２５０は、課金情報テーブル検索部２３０から取得した第１の復号秘密鍵をユーザ処理装置１００に送信する。

ステップ５０７）　ユーザ処理装置１００の復号部１３０は、課金センタ２００から受信した第１の復号秘密鍵を用いて、次に実行する命令を読み出す。

【００７６】ステップ５０８）　復号部１３０は、読み出した命令を復号する。

ステップ５０９）　復号部１３０により復号された命令を実行する。

ステップ５０８とステップ５０９の処理を当該復号され

た命令の全てが終了するまで繰り返す。

【００７７】［第６の実施例］図１２は、本発明の第６の実施例のユーザ処理装置の構成を示す。同図において、図３と同一構成部分には、同一符号を付し、その説明を省略する。なお、本実施例は、図３の構成と同様である。

【００７８】図１２において、ユーザ処理装置１００は、図３の構成に、復号部１３０で復号された命令を格納する復号済ソフトウェア格納部１８０と、当該復号済ソフトウェア格納部１８０に格納されている命令を順次読み出して実行する実行部１９０が付加されたものである。

【００７９】図１３は、本発明の第６の実施例の動作を説明するための図である。

ステップ６０１）　ユーザ処理装置１００において、予め命令部分が暗号化されたソフトウェア１１０を起動する。

ステップ６０２）　ユーザ処理装置１００は、ソフトウェア１００をロードする。

【００８０】ステップ６０３）　ユーザ処理装置１００の課金センタ送信部１２０は、ソフトウェアＩＤ，被課金者ＩＤとを課金センタ２００に送信する。

ステップ６０４）　課金センタ２００の課金情報テーブル検索部２３０は、ユーザ処理装置１００から受信したソフトウェアＩＤを用いて課金情報テーブル２１０を検索し、当該ソフトウェアの使用料と、第１の復号秘密鍵とを取得する。

【００８１】ステップ６０５）　ユーザ課金情報更新部２４０は、ユーザ処理装置１００から受信した被課金者ＩＤを用いてユーザ情報テーブル２２０を検索し、被課金者のユーザ課金情報を課金情報テーブル２１０から取得したソフトウェア使用料で更新する。

【００８２】ステップ６０６）　ユーザ処理装置送信部２５０は、課金情報テーブル検索部２３０から取得した第１の復号秘密鍵をユーザ処理装置１００に送信する。

ステップ６０７）　ユーザ処理装置１００の復号部１３０は、課金センタ２００から受信した第１の復号秘密鍵を用いて、ソフトウェアの全部または、一部の暗号化されている領域を復号する。

【００８３】ステップ６０８）　復号部１３０は、復号したソフトウェアを復号済ソフトウェア格納部１８０に格納する。

ステップ６０９）　実行部１９０は、復号済ソフトウェア格納部１８０にアクセスし、復号されたソフトウェアを実行する。

【００８４】［第７の実施例］本実施例における課金情報テーブル２１０は、ソフトウェアＩＤ、機能に対応した機能ＩＤ，機能に対応した使用量と、機能に対応し、暗号化されているソフトウェアの全部又は一部の領域として復号するための第４の復号・秘密鍵とを含むもの構成である。第４の復号・秘密鍵は、ユーザ処理装置１００に送信され、ソフトウェア１１０を復号するための鍵である。

【００８５】図１４は、本発明の第７の実施例の動作を説明するための図である。

ステップ７０１）　ユーザ処理装置１００は、予め機能毎に異なる秘密鍵を用いて暗号化されたソフトウェアを起動する。

ステップ７０２）　起動したソフトウェアをメモリ上にロードする。

【００８６】ステップ７０３）　ユーザ処理装置１００の課金センタ送信部１２０は、実行しようとする機能の機能ＩＤ（機能Ａ）と、ソフトウェアＩＤと、被課金者ＩＤとを課金センタ２００に送信する。

ステップ７０４）　課金センタ２００の課金情報テーブル検索部２３０は、ユーザ処理装置から受信したソフトウェアＩＤと、機能ＩＤとを用いて、課金情報テーブル２１０を検索し、当該機能の使用料と、第４の復号秘密鍵を取得する。

【００８７】ステップ７０５）　ユーザ課金情報更新部２４０は、課金情報テーブル検索部２３０により取得された機能使用料でユーザ情報テーブル２２０を更新する。

ステップ７０６）　ユーザ処理装置送信部２５０は、課金情報テーブル２１０から取得した第１の復号秘密鍵をユーザ処理装置１００に送信する。

【００８８】ステップ７０７）　ユーザ処理装置１００は、課金センタ２００から受信した第１の復号秘密鍵を用いて、当該機能の全部または、一部の暗号化されているソフトウェアの領域を復号して実行する。上記の手順を、当該ソフトウェアを使用してユーザが必要とする処理が終了するまで、機能の単位で繰り返す。ステップ７０８以降は、ユーザ処理装置１００から機能ＩＤとして“機能Ｂ”を課金センタ２００に送信して、上記のステップ７０４～ステップ７０７と同様の処理を繰り返すものである。

【００８９】なお、上記の各実施例において、ユーザ課金情報としては、前納方式、後納方式、累積課金方式、明細課金方式及びクレジット支払い方式のいずれにも適用可能である。また、上記の各実施例において、ソフトウェアをプログラムとして説明しているが、この例に限定されることなく、プログラムに留まらず、音声情報、映像除法、画像情報、テキスト情報を含む全てのディジタル情報に対して適用可能である。

【００９０】なお、本発明は、上記の実施例に限定されることなく、特許請求の範囲内で種々変更・応用が可能である。

【００９１】

【発明の効果】上述のように、本発明のソフトウェア課金方法及びシステムによれば、どの時点においても暗号

化されている部分を含まないソフトウェアが、メモリ及びディスク等の記憶媒体上に存在しないため、ソフトウェアの反復使用を確実に阻止することができ、ソフトウェアの使用の都度、確実に使用料を徴収することが可能となるため、ユーザは必要な機能のみを安価な使用料で使用することが可能となる。

【００９２】また、ソフトウェアの暗号化に用いる秘密鍵の個数と暗号化の範囲を選択することにより、起動するソフトウェアの単位で課金することも、起動するソフトウェア内の機能群単位に課金することも可能となる。また、使用料前払い、または、使用限度額に基づくクレジットを課金センタに登録して使用料残高を管理することにより、使用料の徴収漏れを防止することが可能となる。

【００９３】また、ユーザ処理装置から課金センタに送信する時に添付した、乱数と課金センタからユーザ処理装置に送信する時に添付された乱数との一致を検証することにより、課金センタからユーザ処理装置に送信された情報を横取りすることによるソフトウェアの不正使用を防止することが可能となる。

【００９４】また、課金センタからユーザ処理装置に送信において、公開暗号方式を利用し、署名を添付することにより、他人の被課金者ＩＤを使用したソフトウェアの不正使用を防止することが可能となる。

【図面の簡単な説明】

【図１】本発明の原理を説明するための図である。

【図２】本発明の原理構成図である。

【図３】本発明のシステム構成図である。

【図４】本発明の第１の実施例の動作を説明するための図である。

【図５】本発明の第２の実施例のシステム構成図である。

【図６】本発明の第２の実施例の動作を説明するための図である。

【図７】本発明の第３の実施例の動作を説明するための図である。

【図８】本発明の第４の実施例のシステム構成図である。

【図９】本発明の第４の実施例のユーザ課金情報更新部の構成図である。

【図１０】本発明の第４の実施例の動作を説明するための図である。

【図１１】本発明の第５の実施例の動作を説明するための図である。

【図１２】本発明の第６の実施例のユーザ処理装置の構成図である。

【図１３】本発明の第６の実施例の動作を説明するための図である。

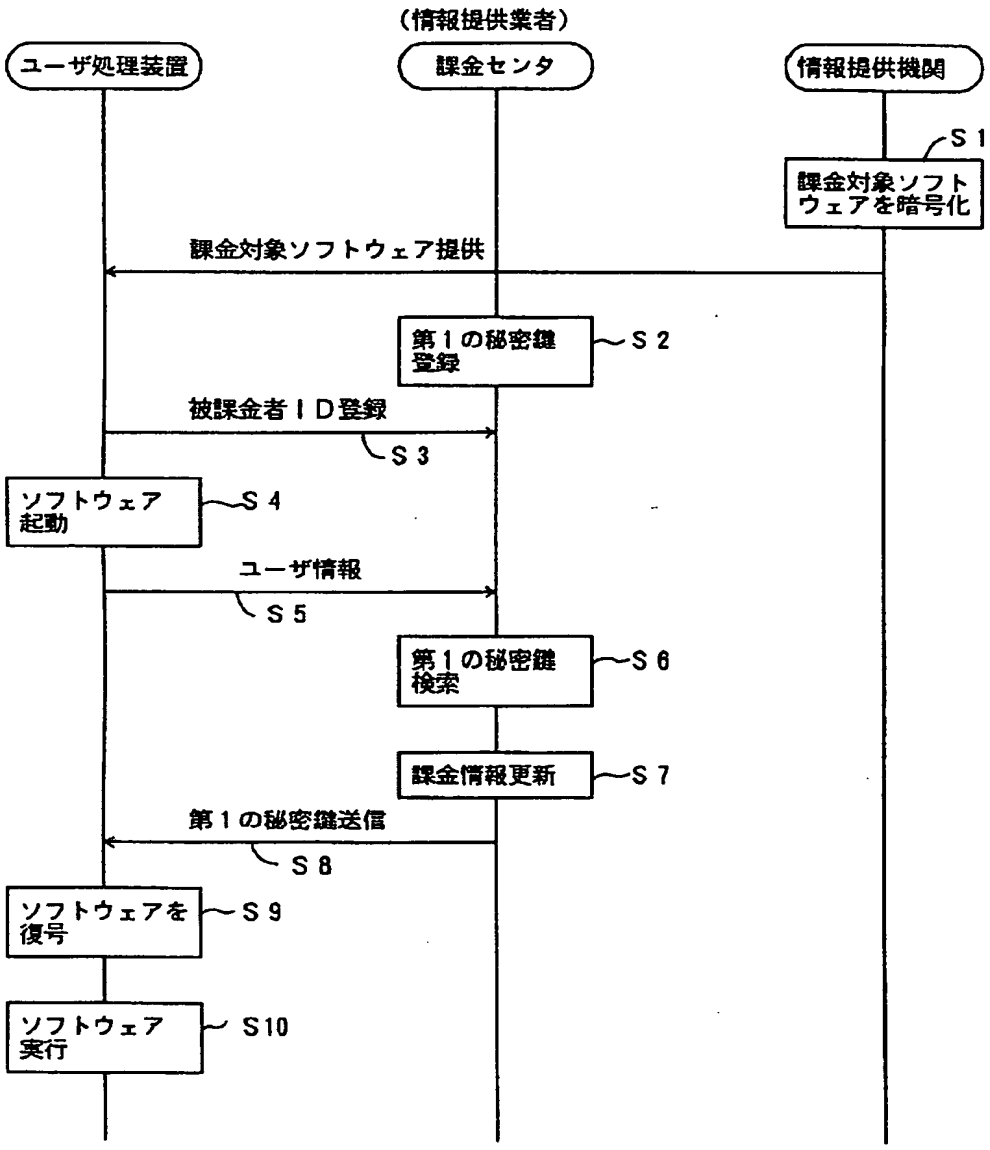
【図１４】本発明の第７の実施例の動作を説明するための図である。

【符号の説明】

１００　ユーザ処理装置
１０１　ＩＤ登録手段
１１０　ソフトウェア
１２０　課金センタ送信部、使用通知手段
１３０　復号部、第１の復号・秘密手段
１４０　乱数生成部
１５０　比較部
１６０　第３の秘密鍵保持部
１７０　署名生成部
１８０　復号済ソフトウェア格納部
１９０　実行部
２００　課金センタ
２０１　第１の暗号化手段
２０２　ソフトウェア提供手段
２１０　課金情報テーブル
２２０　ユーザ情報テーブル
２３０　課金情報テーブル検索部
２４０　ユーザ課金情報更新部、課金手段
２４１　テーブル検索部
２４２　署名復号部
２４３　比較部
２４４　テーブル更新部
２５０　ユーザ処理装置送信部、復号鍵送信手段
２６０　乱数受信部

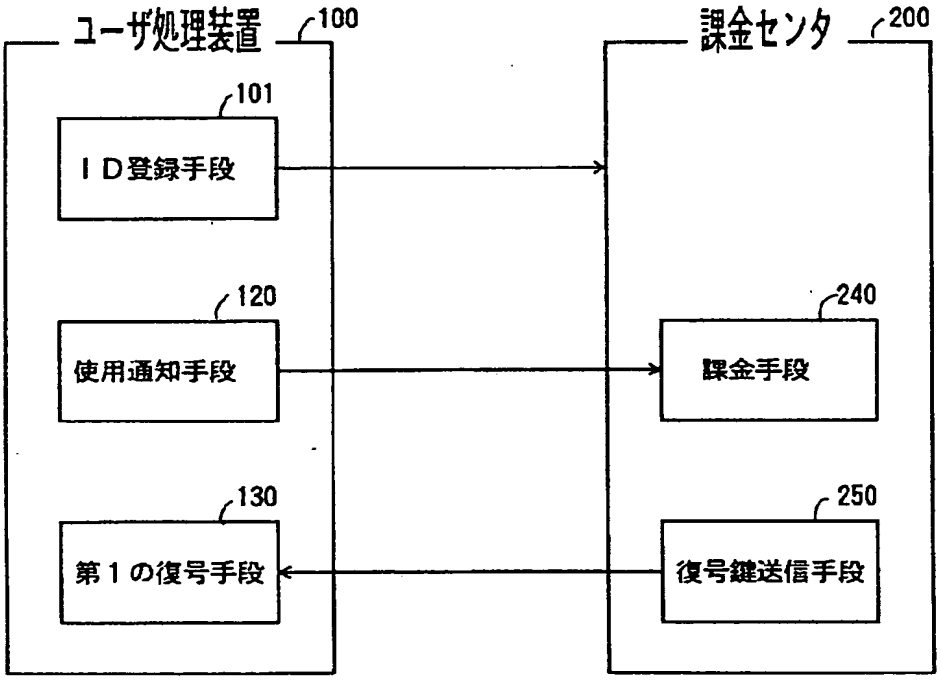
【図１】

本発明の原理を説明するための図



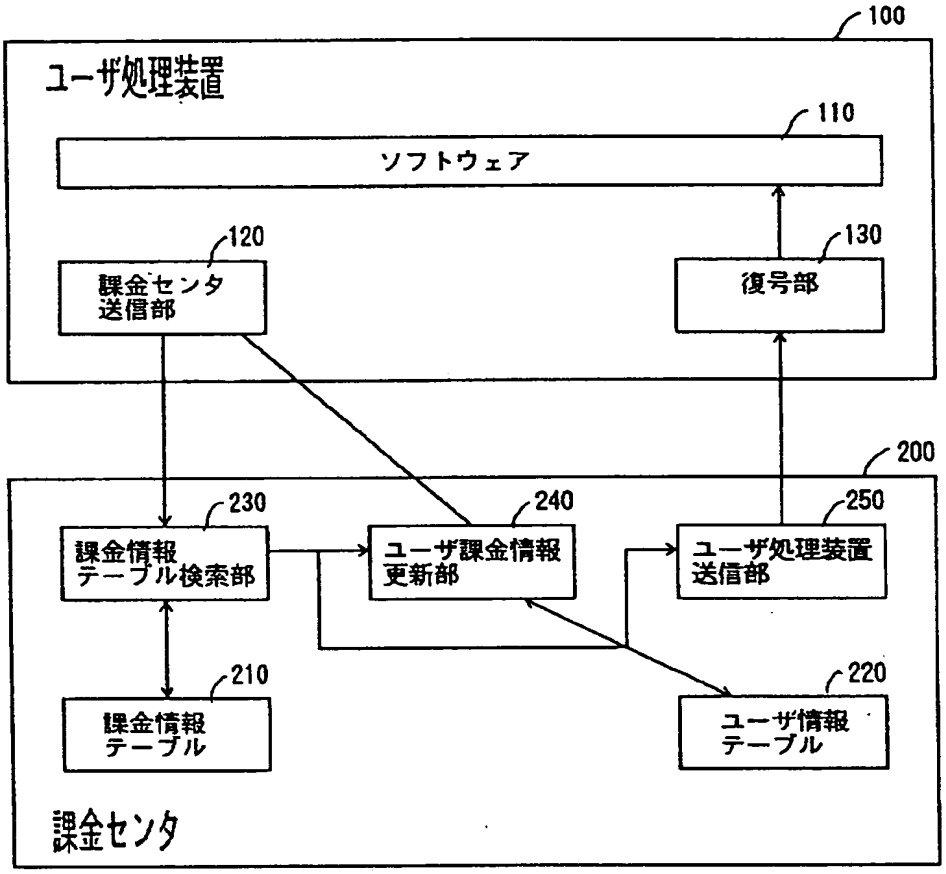
【図２】

本発明の原理構成図



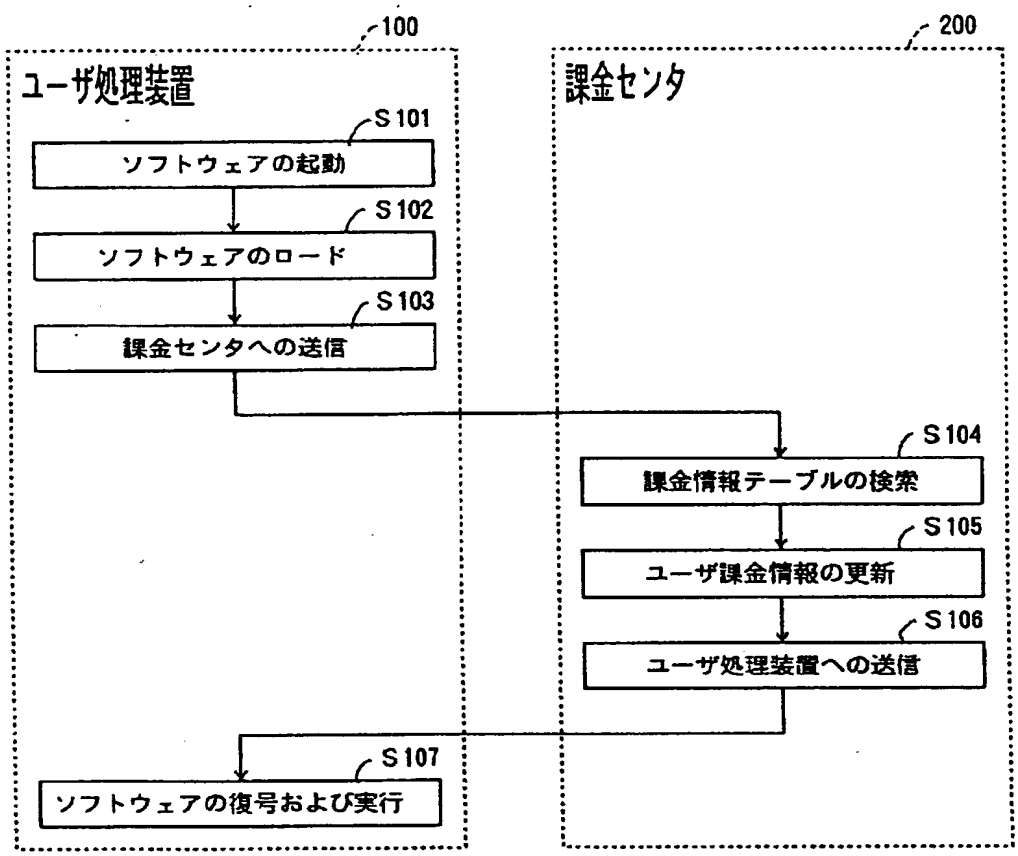
【図３】

本発明のシステム構成図



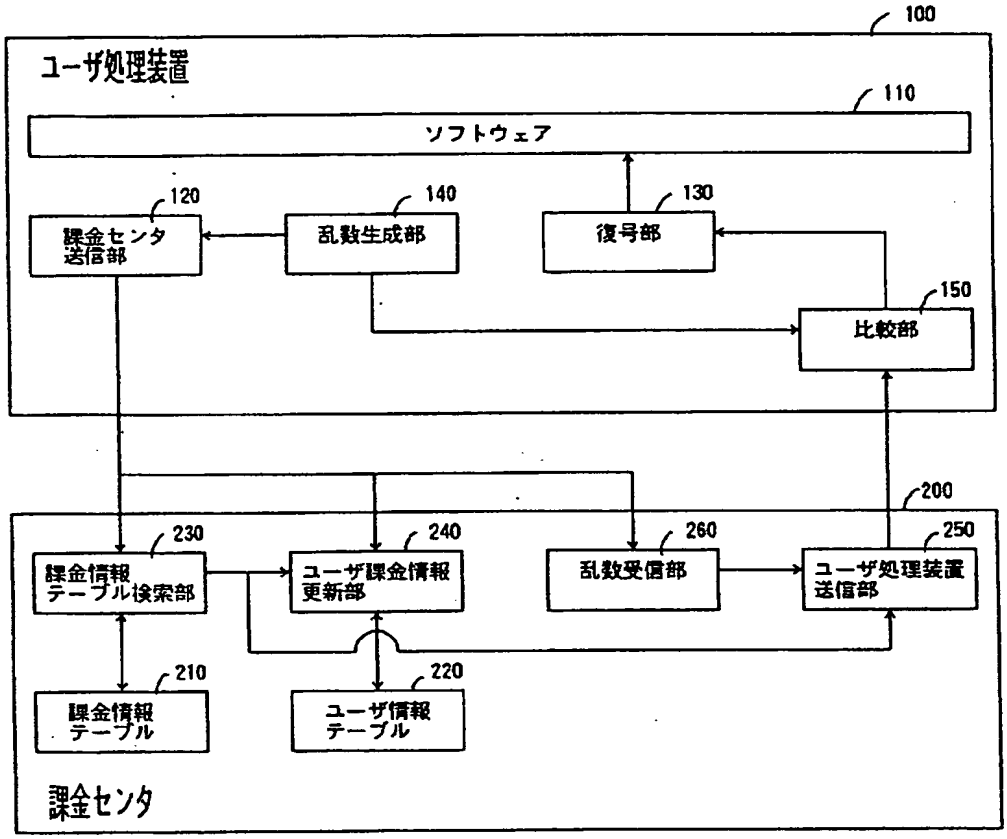
【図４】

本発明の第１の実施例の動作を説明するための図



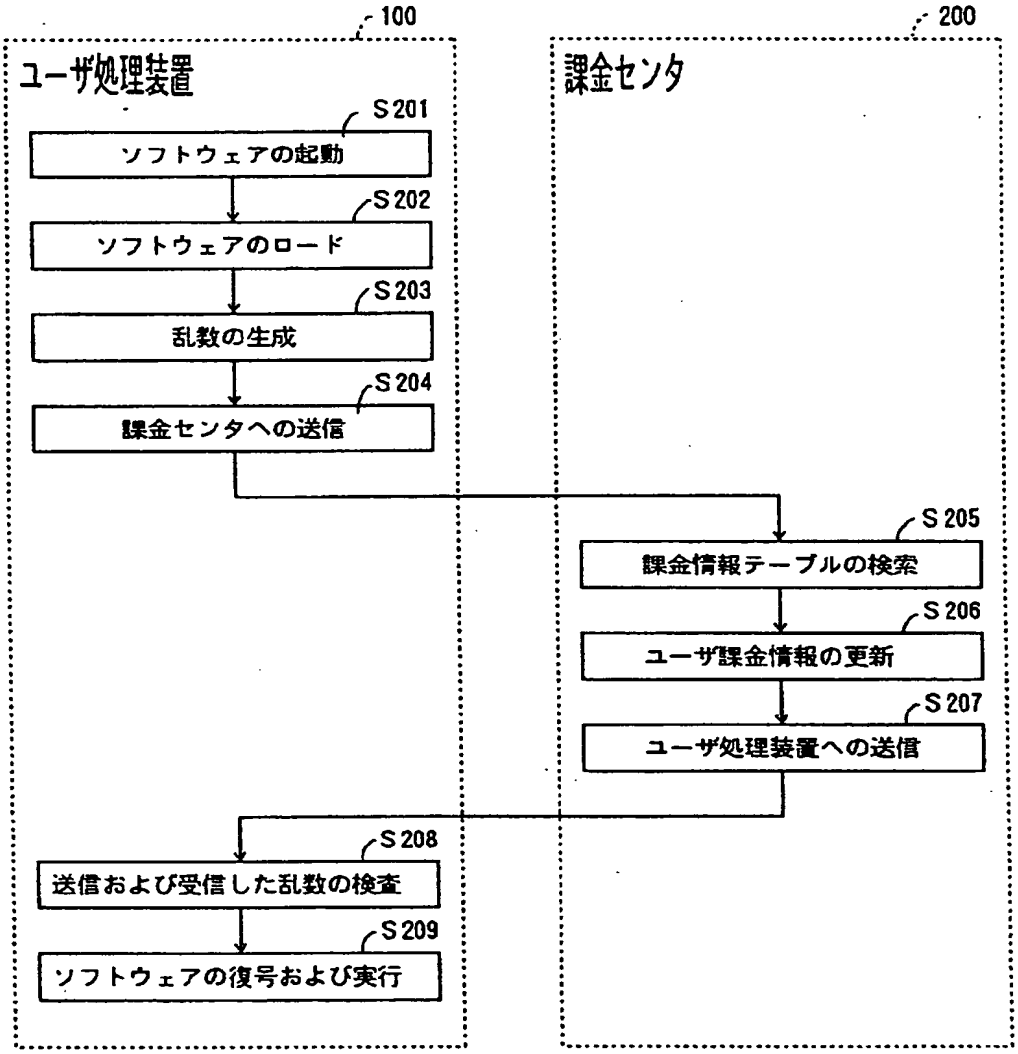
【図５】

本発明の第２の実施例のシステム構成図



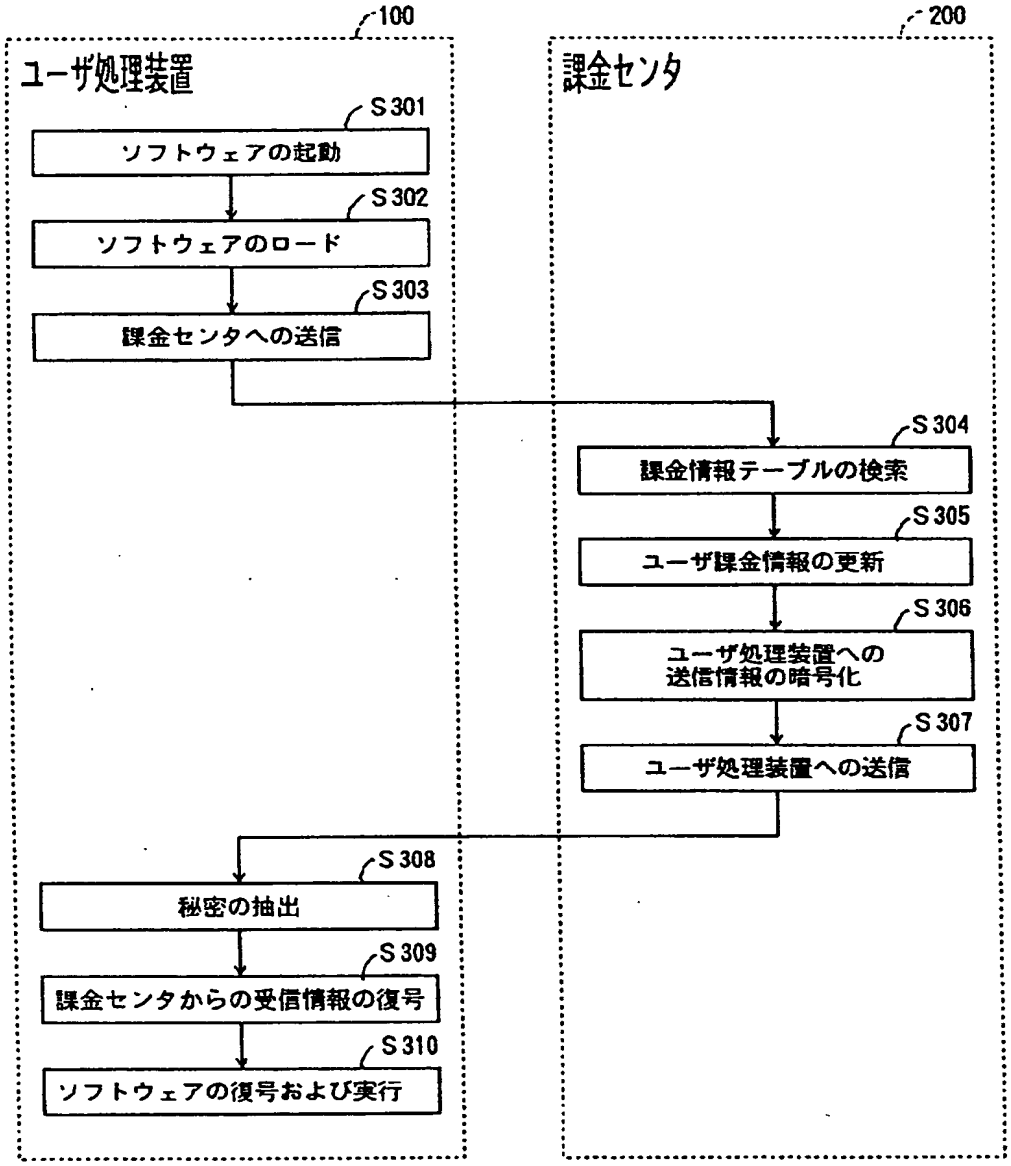
【図６】

本発明の第２の実施例の動作を説明するための図



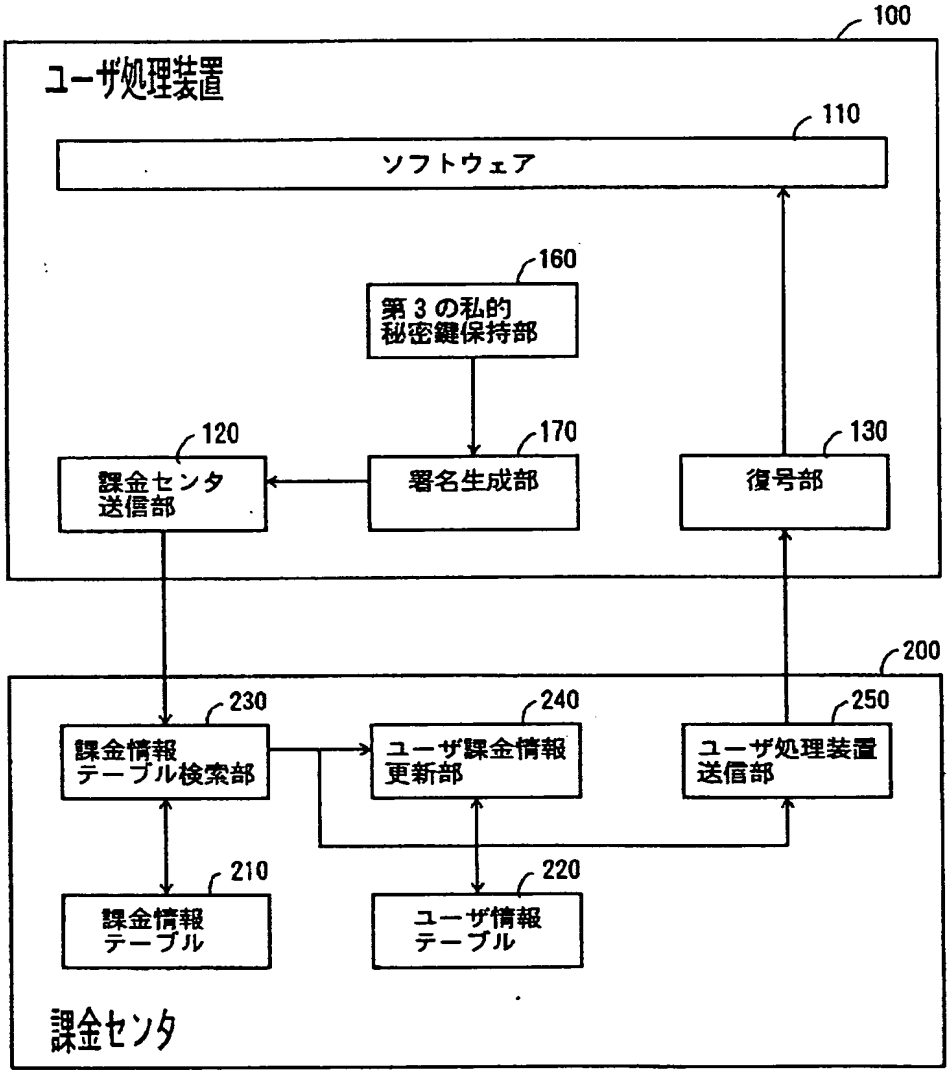
【図７】

本発明の第３の実施例の動作を説明するための図



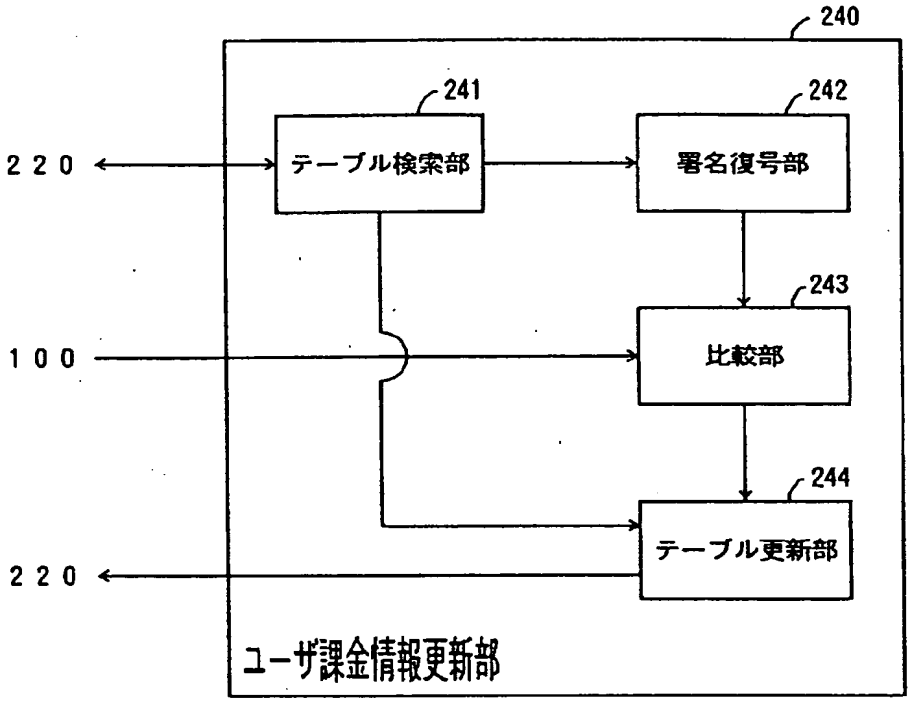
【図８】

本発明の第４の実施例のシステム構成図



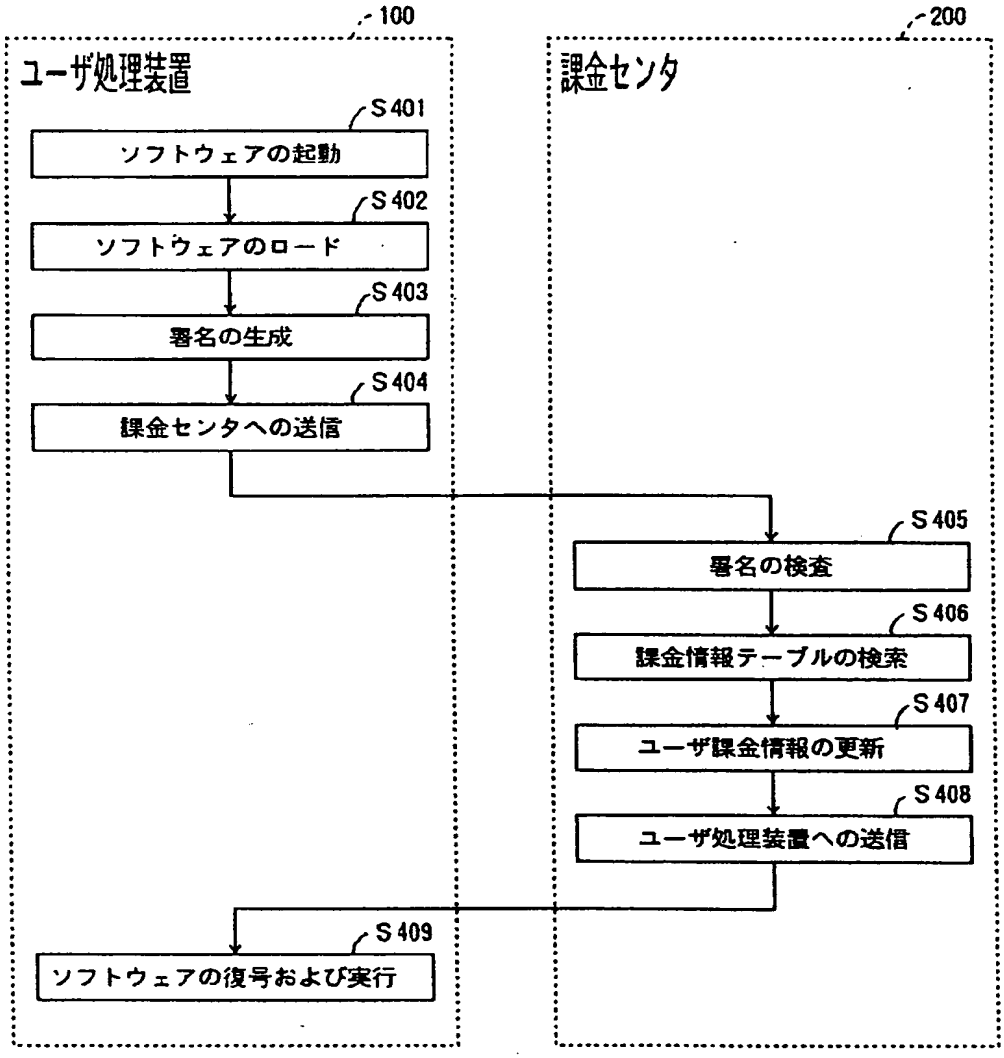
【図９】

本発明の第４の実施例のユーザ課金情報更新部の構成図



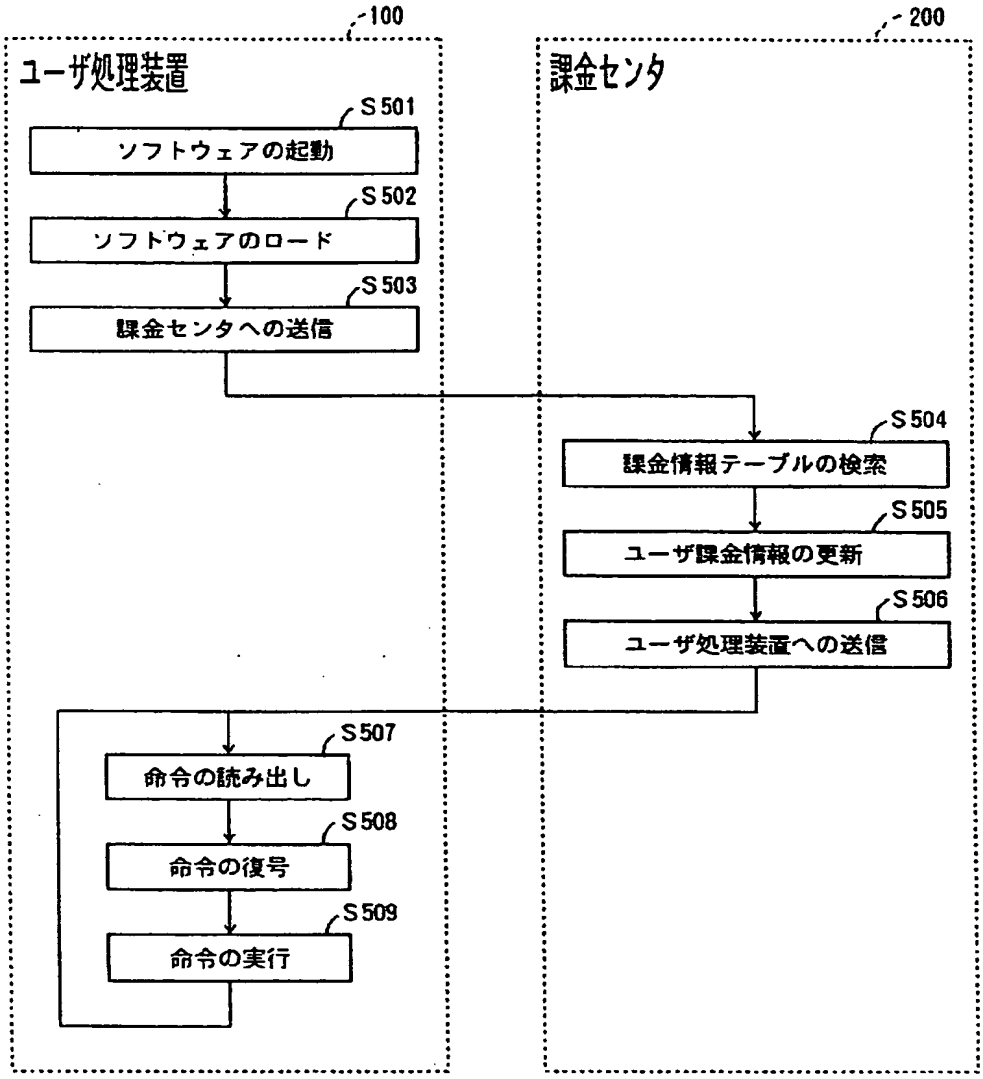
【図１０】

本発明の第４の実施例の動作を説明するための図



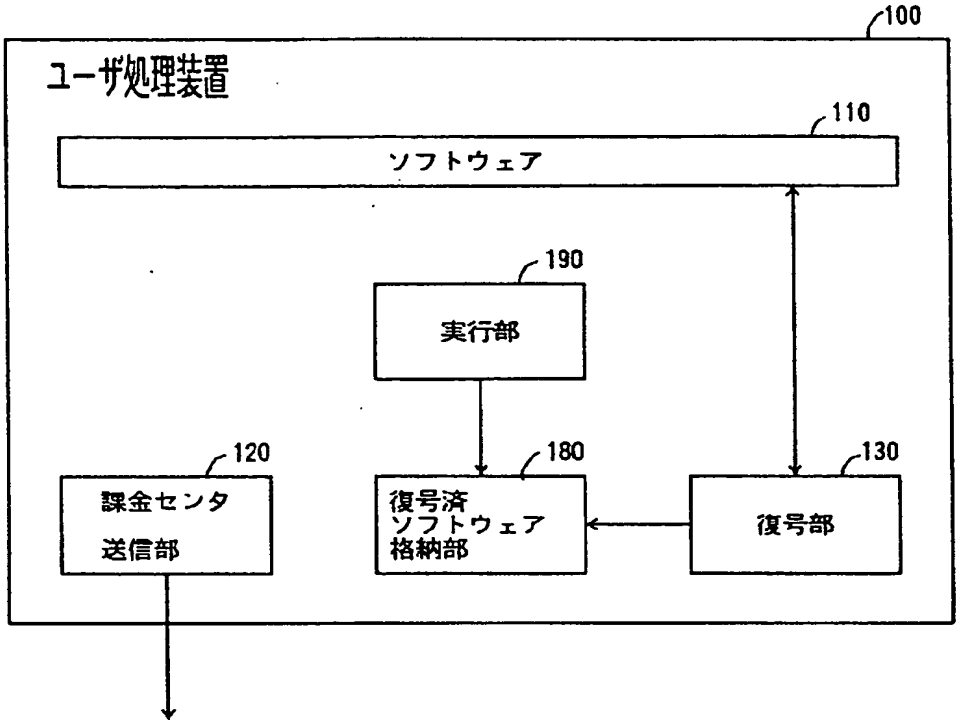
【図１１】

本発明の第５の実施例の動作を説明するための図



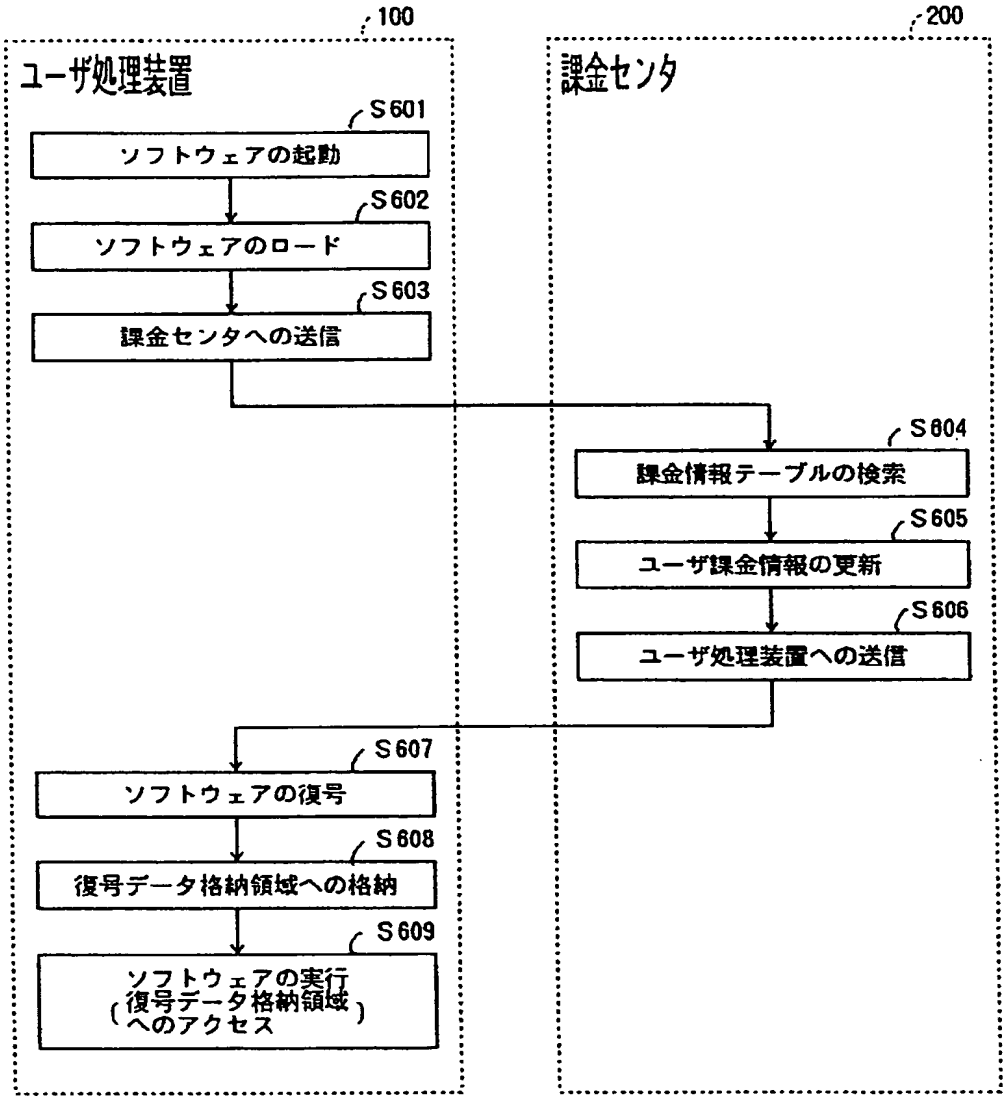
【図１２】

本発明の第６の実施例のユーザ処理装置の構成図



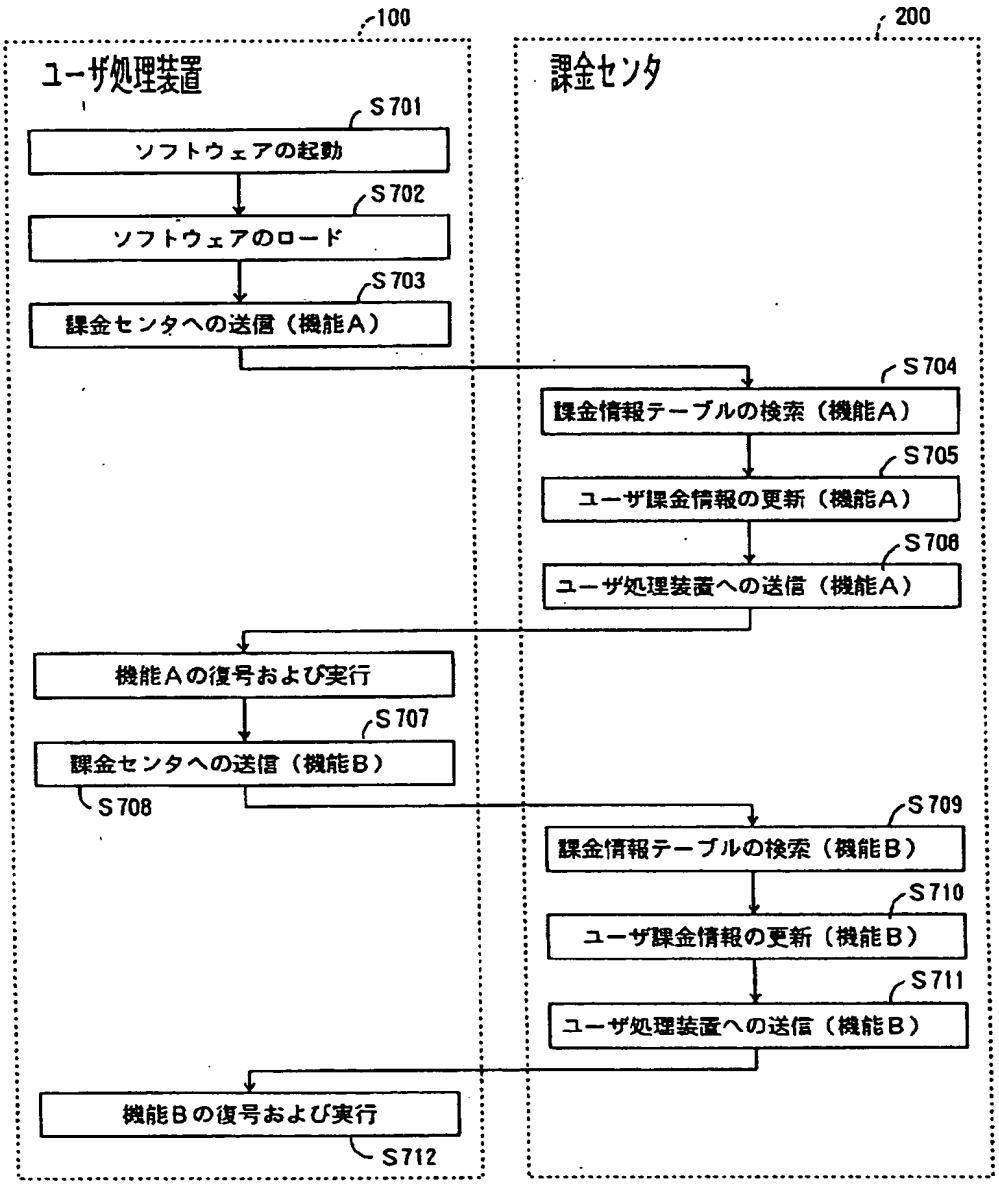
【図１３】

本発明の第６の実施例の動作を説明するための図



【図１４】

本発明の第７の実施例の動作を説明するための図



フロントページの続き

(51)Int.Cl.[6]		識別記号	庁内整理番号	FI		技術表示箇所
G09C	1/00	640	7259－5J	G09C	1/00	640B
			7259－5J			640E
		660	7259－5J			660Z
			7259－5J			660D